2008-01-01

Development of a framework to leverage knowledge management systems to improve security awareness.

Dennis Lupiana
Technological University Dublin, brendan.tierney@tudublin.ie

Development of a Framework to Leverage Knowledge Management Systems to Improve Security Awareness

Dennis Lupiana

A dissertation submitted in partial fulfilment of the requirements of
Dublin Institute of Technology for the degree of
M.Sc. in Computing (Knowledge Management)

September 2008

I certify that this dissertation which I now submit for examination for the award of MSc in Computing (Knowledge Management), is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the test of my work.

This dissertation was prepared according to the regulations for postgraduate study of the Dublin Institute of Technology and has not been submitted in whole or part for an award in any other Institute or University.

The work reported on in this dissertation conforms to the principles and requirements of the Institute's guidelines for ethics in research.

Signed: _____

Date: ***08th September 2008***

ABSTRACT

Security awareness is very essential in securing intellectual property, in particular internal corporate information assets and its "Knowledge". The dynamic nature of security attacks and the need to comply with government policies in protecting organisation's data has a major influence on seeing organisations focus on strengthening against threats from the human element. This is a difficult challenge. Organisations must have a degree of trust their employees. They must trust their employees to interact responsibly as end-users with their information systems. They must trust their employees who work as developers to work responsibly and be motivated to develop systems with the organisations protection in mind. However organisations cannot expect all its employees to be educated in security issues before joining the organisation and therefore must take some responsibility for educating both users and developers on security issues and ethics. Although many organisations do have security policies and awareness programmes, many others don't. Security awareness programmes and policies have varying degrees of success. Therefore the issue of how to improve the security awareness of all employees in organisations, and end-users in particular, is a hot topic.

The project described in this dissertation identified user involvement in highlighting and protecting against security-relevant issues as crucial to ensuring privacy and security of organisational knowledge and corporate information assets. This project investigated how to harness the power of users by developing a framework from which a knowledge management system (KMS) was developed that provides a participatory education approach to security issues. The results of an extensive literature review and the views of security experts and non-experts were used to develop a web based prototype KMS which was evaluated by a group of academic users in higher educational institute in Tanzania. The results of this evaluation were then distributed to security experts and top executives for assessment of using such a KMS to improve security user awareness across the organisation.

Key words: *Computer Systems Security, Security Awareness, Knowledge Management, KMS, KMS-SAWA Framework and Prototype.*

ACKNOWLEDGEMENTS

Foremost, I would like to express my deep and sincere gratitude to my supervisor Ms Deirdre Lawless of the School of Computing at Dublin Institute of Technology. Her wide knowledge in Knowledge Management and logical way of thinking has been of great value to my dissertation.

I would also like to thank Mr. Damian Gordon for his interesting and challenging seminars during the taught part of this course. He has always been more than willing to answer my naïve questions in the preparation of this dissertation and acted as a good friend along the way.

I would also like to thank Dr. Fred J. Mtenzi for his never ending encouragement and support from day one in Ireland. Throughout this course and especially during the project time he has been a source of encouragement and support of all kinds.

Finally, I would also like to express my deep appreciation to my parents. Their continuous support throughout the course has inspired me with confidence, patience and persistence to successful accomplish the course.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1 INTRODUCTION

1.1 Background

Organisational information architectures are becoming increasingly more complex. This need for complexity introduces more bugs that can be exploited to breach corporate security. High demand for system interoperability and so called user friendly interfaces has introduced a new layer of threats and attacks to modern information systems architectures. In addition, the openness of Internet has brought new challenges in protecting organisations' intellectual property and information assets (Herold 2005). Organisations are also constantly busy acquiring the so called sophisticated security tools and applications to fight against these threats (D'Arcy & Hovav 2007). However, technology is unpredictable parameter and relying on technological assistance for security is not sufficient. The focus should be wider and the least organisations can do to control information systems security is to interweave what they already know, *knowledge sharing,* to assist with improving organisational security informing all members of the organisation.

The tight technological security controls that are being deployed within organisations have changed attackers' attention to end-users who are mostly not aware or ignorant of security measures (Smith 2003). Though software developers also pose a big threat in computer security, this dissertation will only concentrate with end-users. With software security paradigm, developers are much away in security ethics than end-users (McGraw 2004). Therefore, in this dissertation end-users are considered more susceptible and therefore pose a significant point of danger when considering protecting organisations' intellectual property and information assets. To at least control the danger from the growing nature of digital threats, increased focus should be directed to human element, in particular end-users. Good users' understanding on security principles is a stepping stone for the successfulness of security measures and organisation as well (Arce 2003; Trcek 2006).

However it is not as simple as just introducing education programme, the challenges remain on how to determine what users require to be aware of, and how to integrate

and make accessible security experts' knowledge to all end-users within the organisation without affecting their productivity. The approach adopted in this project builds on the definition that Knowledge Management System (KMS) is an information system that aims to facilitate the codification, collection, integration, and dissemination of organisational knowledge (Bernard 2006). As such the project aims to investigate where using a KMS could assist with improving security awareness. In this dissertation, the KMS developed plays dual roles, firstly to store and communicate security related knowledge contents and secondly to allow users to compare their security-relevant activities with security policies and to either suggest on security policy amendments or additions to training programmes.

1.2 Research problem

Many researchers emphasise on the involvement of employees in security awareness programme (Chia, Maynard & Ruighaver 2002; Desman 2002; Herold 2005). On the other hand, central to the improvement of organisational performance is employees' contributions.

Therefore, since KM recognises the contributions employees have in improving organisational performance, this project will investigate possible KM processes and KMS features to improve organisational security awareness.

The primary aim of this project was to investigate users' awareness in security issues and the usefulness of KMS in improving security user awareness thereafter to develop a framework that leverages KMS in improving security awareness in an organisational context. From this framework a prototype KMS is developed.

1.3 Intellectual challenge

To achieve the aim of this project, an investigation of the roles of users play in computer security and security awareness was necessary so as to build insights on the trend of computer threats as associated with users, and the efforts organisations undertake to equip their users with necessary skills to fight against these threats.

Moreover, an investigation on Knowledge Management was conducted to ascertain the possible knowledge activities that are appropriate in improving users' awareness in computer security related issues and the fundamental characteristics of KMS, their usage and implementation requirements. An investigation of KMS was conducted to assess their feasibility in improving security awareness in an organisational context. Following this investigation, appropriate features of KMS were highlighted for the improvement of users' security awareness.

Finally, building on highlighted features of KMS, a Wiki based prototype was developed to assess the contributions of KMS in improving users' security awareness.

1.4 Research objectives

The following objectives have been achieved throughout the dissertation and contributed to the overall outcome:

1. **Review of computer security and security awareness approaches.**
   An extensive literature review of computer security and security awareness approaches was conducted to analyse the trend of computer threats regarding to users and the efforts organisations undertook in educating users.
2. **Investigate users' involvement in computer security.**
   An investigation of users' involvement in computer security was conducted to analyse the roles users play in computer security. To accomplish this, the survey was created based on the results of a literature review of computer security and security awareness.
3. **Investigate Knowledge Management and KMS.**
   An extensive literature review on Knowledge Management and KMS was conducted to analyse their feasibility in improving security awareness.
4. **Develop a framework for implementing KMS to improve security awareness**
   An open framework was developed to assist organisations when implementing KMS to improve security awareness. The framework was evaluated by security experts to analyse its applicability within an organisational context.

5. **Develop and evaluate a Knowledge Management System prototype.**
   A Wiki based KMS was developed to assess the contributions of KMS in improving security awareness. The prototype was then evaluated by both security experts and end-users.

1.5 Research methodology

To successful accomplish the above objectives both primary and secondary research was conducted. Primary research included both questionnaires and interviews. Secondary research concentrated on extensive literature review.

Beginning with the secondary research, an extensive literature review was conducted in the field of computer security and security awareness to investigate current situations on computer threats as associated with users and the efforts organisations undertake to educate their users.

Following the results obtained from the literature review of computer security and security awareness, a primary research was conducted to investigate the roles users play in computer security and the contributions of current security awareness programmes into educating users.

This primary research was questionnaire-based survey covering many countries in the world. The targeted audiences were security experts and organisational users. The survey involved both physical distribution of questionnaires and online survey. Thereafter an interview with security experts was conducted to evaluate the findings.

Parallel to security awareness survey, an extensive literature review on Knowledge Management and KMS was also conducted to ascertain appropriate knowledge management activities and key features of KMS that can be useful in improving security awareness.

Following the results from literature reviews and security awareness survey, security awareness was mapped as a knowledge management problem. Thereafter, a framework was developed to guide organisations in building KMS for improving security

awareness. To evaluate the applicability of the framework, an interview with security experts was conducted.

Finally, a KMS prototype was developed using Wiki collaborative tool. Security experts were invited to evaluate its implementation process by suggesting on the look and feel of its contents. Thereafter users, specifically from Africa, were invited to participate in the Wiki for a period of two weeks and thereafter to evaluate its contribution on users' understanding on computer security issues.

1.6 Resources

To successful accomplish this project both technical and non-technical resources were essential. Below is the list and briefly explanation of each category:

- **Technical resources**

1. *Personal computer*

   Availability of personal computer, specifically laptop, with full installed word processing and analytical applications was essential for the documentation of this dissertation.

2. *Online survey tool*

   Accessibility of online survey tool, http://www.group-surveys.com, was also essential in successful accomplishment of this project. The tool was useful in conducting online survey.

3. *Online Wiki tool*

   Accessibility of online Wiki tool, http://kms-sawa.wetpaint.com, was necessary for the successful accomplishment of this project. The tool was useful on the development of Knowledge Management System prototype.

4. *Internet access*

   Accessibility to internet was vital on the completion of this project. Besides its facilitation in literature survey, internet acted as focal resource for the successful completion of this project. Firstly, it assisted in routine communications with project supervisor, and security experts. It also acted as access point for online survey and Wiki tools.

- **Non-technical resources**

  1. *Library access*

     Access to library facilities was necessary for the successful completion of this project for conducting extensive literature survey. This included both physical and online accessibility. Physical accessibility was for literature reviewing on books and previous dissertations, while online was useful for accessibility of electronic journals.

  2. *Industrial contacts*

     Accessibility of industrial contacts for security experts was necessary throughout this project to assist in the evaluation of survey results, framework and KM System prototype.

  3. *Project Supervisor*

     Accessibility to project supervisor was vital for successful completion of this project. Project Supervisor was on the centre of this project by providing access to security experts who played central role in this project. Moreover, project supervisor provided assistance in coherence of the document.

1.7 Scope and limitations

The world is so large and is made up of different organisations with different cultures. Finding the true view of security awareness of all organisations could involve an extensive survey and interviews. However, due to time limitation this project focused on a subset of security experts who were accessible and users in Ireland and East Africa. Although the findings cannot be considered definitive for every organisation they still can be considered interesting and useful for those interested in assessing their security awareness. In addition it offers new insights into the current state of security awareness in higher education in East Africa.

1.8 Organisation of the dissertation

The remaining chapters of this research project are organised as follows:

Chapter 2 discusses computer systems security. The aim of this chapter is to investigate the trend of computer security threats and their control measures related to users. The chapter starts by the introduction of the chapter then followed by the discussion of computer systems background. The third section provides the discussion of three key issues in computer systems security. The fourth section provides the discussion of computer systems threats. The last section provides a discussion of three computer systems security controls; technical, management and institutionalisation. The chapter concludes by outlining users' influences in ensuring computer security and the effects of technological control measures.

Chapter 3 focuses on security awareness. The aim of this chapter is to investigate current security awareness programmes and the involvement of users. The chapter starts by the introduction of the chapter then followed by the definition of security user awareness. The third section provides security awareness building process followed by the discussion of current security awareness approaches. The fifth section provides the discussion of security awareness in Ireland followed by the security awareness in Tanzania. The last section provides the review on the failure of the current security awareness.

Chapter 4 focuses on knowledge management systems. The aim of this chapter is to investigate key processes of knowledge management and appropriate features of KMS in improving security awareness. The chapter starts by introducing the chapter then followed by the discussion of knowledge management. The discussion of organisational learning will be provided in section three. Section four provides the discussion of computing for knowledge management. The discussion about KMS will be provided in the fifth section. The chapter concludes by highlighting key knowledge management processes and key KMS features that can be useful in improving security awareness in an organisational context.

Chapter 5 focuses on knowledge management perspectives on security awareness. The aim of this chapter is to show how KMS can be useful in improving security awareness. The chapter starts by the introduction of the chapter then followed by the explanation of why security awareness is a knowledge management problem. The third section provides the discussion of organisational security culture where NIST learning continuum and Microsoft security learning cycle will be discussed.

Chapter 6 provides security awareness survey. The aim of this chapter is to investigate the roles users play in computer security and the effectiveness of current security awareness programmes. The chapter starts by introducing the chapter then followed by the discussion of audiences. The third section provides the discussion of survey methodology. Questionnaire design will be explained in the fourth section followed by the survey results analysis on the fifth section. The sixth section describes supporting interviews then followed by summary of the findings. The chapter concludes by outlining the level of users' involvement in security issues and the effectiveness of current security awareness programmes.

Chapter 7 describes the KMS-SAWA framework and prototype implementation and evaluation process. The chapter will be introduced before the discussion on the factors for the KMS implementation for security awareness. The third section provides the discussion of initial KMS-SAWA framework. The fourth section will provide the KMS-SAWA framework descriptions. Prototype implementation will be described in the fifth section followed by its evaluation process in the sixth section. The chapter concludes by outlining the key benefits of KMS-SAWA framework and KMS has in improving security awareness.

Chapter 8 is the conclusion of the dissertation. The aim of this chapter is to give the reader an overview of the research project by pointing out key elements and suggesting future work. The chapter starts by introducing the chapter then followed by the definition and overview of the research. The third section describes the contributions to the body of knowledge. Experimentation, evaluation and limitations will be explained in section 5 then followed by the suggestion of future work and research. The chapter concludes by outlining key findings of the project and their possible solutions.

2 COMPUTER SYSTEMS SECURITY

2.1 Introduction

There is no doubt on the benefits computer systems and its applications have brought to our life. Large storage space, high processing speed and the pervasive nature of computer systems are among the functionalities that have enabled us to do things which to us were previously unimaginable. The Internet has completely changed the way we communicate. It has made the world in a single village where you can talk and chat all over the world cheaply. E-commerce and its applications have introduced new business opportunities that have attracted a plethora of computer users.

It is now the reality for all organisations, of any size, that the use of computer systems and internet technology is essential to the success of their day-to-day business operations. Unfortunately, all these benefits come with security burden. As technology advances, it brings with it a number of vulnerabilities. The complex nature of applications, the demand for the interoperability of devices and systems, the portable nature of devices and the demand for distributed environments have contributed to making digital life miserable and pose significant challenges for organisations.

Individuals and organisations are now enjoying the evil side of technology. Many technological and managerial controls have been implemented to fight against these evil spirits but still they are suffering. The battle between bad guys and good guys is an endless battle. While one end succeeds, the other end changes the tactics. Although the investigation of KMS to improve security awareness is the focal point of this dissertation, central to achieving this is establishing a clear picture of what exactly is involved in computer security, examining the issues from a number of perspectives. You can only with the battle when you know how your opponent operates.

This chapter presents a short review of computer security and its evolution to become a mainstream topic of importance to all organisations. The variety and complexity of issues which fall under the umbrella of computer security are discussed and the challenges they present to organisations are assessed from an organisational

perspective. The chapter concludes by identifying the security issues which are recognised in the literature as those of most importance to modern organisations.

2.2 Computer systems background

In their very beginning, computers where meant to handle well-structured jobs such as scientific or transaction calculations that were difficult for human beings (S. Gupta & Mccabe 1987). These computers were built by vacuum tubes; they were very huge in size and their speeds were relatively slow. Those were the days when multitasking was merely a nightmare and the only interactions with computers were through punched cards (Lubbes 1993). During those days, computer security was not a headache; the main concern was physical security of computer room. Table 1 presents the summary for computer systems evolution.

	Hardware		Software		
Generation	**Technology**	**Example Systems**	**Methodology**	**Examples**	**Principal kind of Data Handled**
1st Generation 1950's	Vacuum tubes	ENIAC, WHIRLWIND	Binary	0,1 (machine specific)	Binary numbers
2nd Generation Early 1960's	Transistors	IBM 709	Assembly	Assembly (machine specific)	numbers
3rd Generation Late 1960's	Integrated circuits	PDP 11	High-level languages	FORTRAN, Pascal, PL/1	Numbers and some text
4th Generation 1970's	Large scale integration	IBM 370; AMDAHL 470	Elementary information systems	IMS, SQL	Numbers, text
5th Generation Mid-1980's	Hardware implementation of traditional software functions, truly user-friendly systems	Yet to come	High level decision support systems	Yet to come	Number, text, video

Table 1: Five Generations of Computers

(Adapted from (A. Gupta & Toong 1984))

As shown in table 1, the second generation of computer systems was built on transistors. However, this turned out to be unsuccessful because the acquisition cost was relatively high. This led to the emergence of new breed of computer systems. In 1960s, the third computer generation was introduced. Computers in this generation were built with small scale integrated circuits where one "IC" replaced several transistors (Tanenbaum 2008, p.13). This was relatively cheap and attracted more people into the world of digital life. Despite of its acquisition cost, computers in this generation came along with a lot of magic. Multiprogramming, spooling and multitasking are among these wonders which provide a comfortable room for networking.

Unfortunately, technology is not stagnant. The more wonders it brings, the more insecure we are. In early 1970s, when microprocessors were introduced, things started to slip. The ability to compress multiple functions into a single chip enabled personal computers to be built at lower costs that were affordable to almost everyone (A. Gupta & Toong 1984). Besides attracting many users, it also introduced another layer of security threats; device malfunctioning. This was the era of *fault-tolerance* where system availability was measured based on the cost of the system and its functional criticality (Siewiorek & Swarz 1998, p.4). .

Moreover, as the main memory and processor speed increased, the demand for more functionality also increased (S. Gupta & Mccabe 1987). This resulted to more complex application programs with thousands of line of codes. Unfortunately, as applications grow in line of codes, chances of having software bugs also increases (Tanenbaum 2008, p.11). It is through the exploitation of these bugs that attackers are able to launch their attacks. In fact, above all these threats, with exception of social engineering, software bugs are the catalysts for attackers' malicious events (McGraw 2004).

As technology advances, computer systems become ever cheaper and hence attract more users who mostly are not necessarily highly computer literate. Things became even worse in 1990s when internet and its twin-brother (WWW) were introduced (Mowery & Simcoe 2002). Together, they brought many benefits that organisations and individuals could not resist. The introduction of e-business, social networks and online gaming have attracted even more users. With the increase in customers,

organisations need to provide their services twenty-four hours. All these had happened so fast to make the issue of security an after thought (Straub & Welke 1998, p.3).

Technology is not stagnant, the more wonders it brings, the more insecure we are. Computer threats evolve the same way as technology evolves. It is because of this technology that our digital life now is miserable. It has engulfed us to the extent we can not retreat and yet it has not promised our safety. Therefore, it now is a crucial moment when knowing what exactly underlies computer security is essential to determine the necessary means of tossing the other side of the coin to ensure improved safety.

2.3 Key Issues in Computer systems security

There is no doubt about the wonders computer systems have brought to our life. Early from its dawn, computer systems enabled us to do scientific calculations that were iron-line to human brains. Those were the days where only few people had a direct access with it. However, technology is not stagnant. As technology began its pace, the cost of building computer systems drastically decreased. This changed the scope of computer systems. Much functionality were demanded to suit the flexibility nature of business. Unfortunately, technology has equal opportunities to anybody. As it advances, it attracted another category of beneficiaries. Therefore, it is now a crucial for organisation to turn their head and consider the negative side of computer systems.

Stallings (2006, p.3) defines computer security as security of computer systems against any malicious events. These events generalise both human intruders and anything that associate with it (Russell & Gangemi 1991, p.8). Furthering the scope of computer security, Andress (2003, p.5) argues that security is a three parameter process; technology, people and process. Technology readiness provides computer security with sophisticated control measures against malicious events. The process determines how security should be exercised within the organisation while people are the one who should practice security principles to ensure computer security.

The discipline of computer security is so wide, it can take years to tackle every niche of it. However, to avoid the trivialness side of it and to welcome the clarity side, this

section will only tackle computer security in three dimensions as proposed by Bishop (2003, p.4). Bishop argues that computer security spans into three concepts; confidentiality, integrity and availability, see figure 1. Therefore, this section will explore the broadness of these concepts in relation to computer security and their effects in organisational context.

Figure 1: Relationship between Confidentiality, Integrity and Availability
(Source: (C. P. Pfleeger & S. L. Pfleeger 2003, p.11))

2.3.1 Confidentiality

The explanation of this aspect differs depending on the context they arise. Bishop (2003, p.4) defines confidentiality as the process of concealing the accessibility of information resources from an unauthorised access while on the other hand, network gurus define confidentiality as a process of concealing the transmitted data from being intercepted by intruders (Stallings 2006, p.18). However, all these definitions have common aim of prevention of unauthorised access to information resources. Due to high sensitivity of their information and need of classified information, military defence is renowned as the antecedent of this aspect (Russell & Gangemi 1991, p.28).

Many researchers argue that the successfulness of organisation relies on how well it utilise its intangible resources to create new ideas and innovations (Alavi 1997; Hahn

& Subramani 2000; Lang 2001; Stenmark 2002). However, they overlooked a crucial bit of protecting these ideas and innovations. For instance, suppose the marketing and sales team of Vodafone had managed to harness whatever their staffs has to come up with a new strategy of cutting down their call rates to attract more customers however security was overlooked and no proper security control measures implemented. Their rival O2 came across the ideas and launched the offer before they could. What do you think will happen, will Vodafone still execute their strategy as they expected?

This concludes that the issue of confidentiality is not only a military issue. As it is badly required by military to protect their missiles' technology, so are financial and other organisations in protecting their intellectual properties (Randeree 2006; Cole et al. 2008). This emphasises that for any organisation to be successful it should know how to leverage what employees' have as well as to provide necessary protection to their intelligence. Unfortunately, many of mechanisms to ensure confidentiality relies on human being who are required to secretly handle their account passwords or an encryption key .

Moreover, the issue of confidentiality has gained more popularity in the domain of medicine (Siegler 2006). The demand for improving effectiveness and efficiency of health care services by providing a lifelong storage, twenty-four hours and public access of patients' records have came along with risks of confidentiality of patients' information (McClelland & Thomas 2002). All these come by introducing sophisticated technologies that needs to be operated by professionals who are not native of medical domain (Siegler 2006, p.598).

However, this does not mean that other organisations are safe from confidentiality issue. Other organisations like financial institutions, education, transportation, and any organisations, are the victims of system failures, data and money theft and all sorts of evils due to failure of enforcing confidentiality. Military, Telecommunication and Medicine organisations have been used in this section to elaborate the danger that might occur due to violation of confidentiality.

2.3.2 Integrity

If we can not guarantee the confidentiality of sensitive information at least we have to validate the originality of that information. According to Janczewski and Colarik (2005, p.2) data integrity is protecting message from unauthorised modifications. Moreover, Caroll (1996, pp.369-374) defines data integrity as assurance of the trustworthiness of data. This is very essential attribute when it comes to internet and data storage as well. Customers need to be sure of what they send and receive through the communication channel while on the other hand financial institutions focus on data error cleaning to reduce noisy data.

Moreover, Zhou and Haas (1999) argue that message integrity can be violated by "radio propagation impairment" and malicious attacks. However, for the purpose of this dissertation, only violations based on malicious attacks will be considered. Working with integrity is different from working with confidentiality. In confidentiality the data is either compromised or not, but in integrity it involves the correctness of the data; from whom the information is from, how well the data was handled before reaching destination machine and how is being protected in the current machine (Bishop 2003, p.5).

However, it is very difficult to guarantee data trustworthiness with human element (Lee et al. 2002). The field of integrity is also very active in database management systems (DBMS) and data mining as well. In DBMS, failure to record a correct entry can have a big effect to organisation. For instance, if a "Store Keeper" wants to order new computers for organisation "A" and instead of writing 50, unconsciously she writes 500. This can cause a loss of large amount of money to her organisation. Moreover, data error is a hot topic in data mining. Failure of cleansing data in data mining can result to instability of predicted models (Maletic & Marcus 2000). All these scenarios emphasises the danger human element can violate integrity.

2.3.3 Availability

Availability goes the other way around of confidentiality. Confidentiality focuses on limiting data availability while on the other hand, availability strives to make data available (C. P. Pfleeger & S. L. Pfleeger 2003, p.12). Therefore, building on that view

there must be a balance between these two. However, availability stretches to both the system itself and the data in it. On system side, availability means the system is fully operational while on the data side, availability means more than just available for use (C. P. Pfleeger & S. L. Pfleeger 2003, p.12). It goes beyond to consider the response time and fairness between requesters. The former consider the time taken from the time the request was made to the time the data was retrieved. The latter considers the biasness of resource allocation between requesters.

However, many researchers have defined availability differently. Bishop (2003, p.6) defines availability as the ability to request and use the systems and resources as desired. Moreover, Janczewski and Colarik (2005, p.2) defines availability as the protection of intruders from withholding of information and resources. Regardless to the meaning of definitions, they all emphasise on convenient environment with no or minimal system downtime.

2.3.4 Confidentiality, Integrity, Availability

Confidentiality, Integrity and Availability are core elements of computer security and yet human element is the centre of all these. Employees are expected to keep their password confidential and yet they may be required to share with colleagues. On the other hand network administrators are required to carefully analyse network traffic and yet they ignore it. Moreover, clerks are expected to correctly record data entries, but yet they either forget or intentionally record them incorrectly. All these intentionally and unintentionally decisions that humans makes have huge impact to organisation prosperity.

2.4 Computer systems threats

As previously mentioned, technology is the engineer of all these threats. It is egocentric to deny the benefit technology has brought us. Unfortunately it is this technology that made computer attacks evolved from physical to remote attacks. Now we hear many new terms describing different types of attacks that are out there. Terminologies like *crimeware*, *malware*, *driven-by-downloads* attacks, *man-in-the-middle* and many alike have filled the air of digital world. All these terminologies reflect the increase in vulnerabilities and computer threats as well.

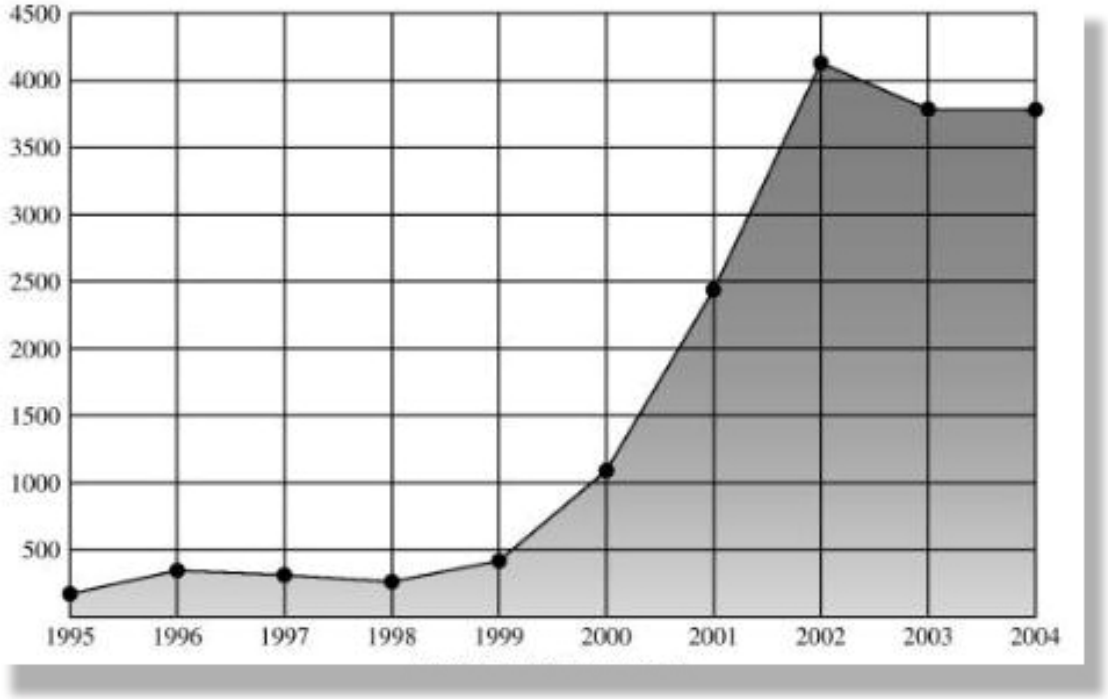

Figure 2: Trend of internet vulnerabilities
(Adapted from (Stallings 2006, p.10))

As it can be shown on figure 2, in 1995 where internet technology was in its embryonic stage, the numbers of vulnerabilities were minimal. However, as years are piling and demands for more functionalities increases, things are getting even worst. As it can be shown from figure 2, number of vulnerabilities increases with the increase of years.

However, prior to explanation of computer threats it is worthwhile explaining the jargons that are associated with it. These include threats and vulnerabilities. Bishop (2003, p.6) defines threat as a possibility for vulnerability exploitation. This implies that not necessarily for a threat to occur to be called a threat. On the other side, vulnerability can be defined as the existence of security loophole that if exploited can lead to security breach (Peltier 2005). For instance, the discovery of a bug in a browser which is regarded as vulnerability, in itself is qualified to be a threat even though it has not been exploited already.

2.4.1 Motivation of Computer Attackers

It is trivial knowing the number of computer break-ins without knowing the motivation behind them. Therefore it is worthwhile understanding why computer attackers and cyber-criminals do what they do. What things that motivates them to be as they are. George (2007) proposed three factors that motivate these miscreants to be what they are. Everything we are doing, we do for reasons.

In his descriptions, George (2007) explained three reasons; *acts of damage*, *propaganda* and *recruitment and internal communication platform* as most reasons to why attackers practices evil things. In acts of damage he explained political and financial influences. In propaganda he explained about the art of being recognised and lastly the disgruntled employees. For instance, due to employment termination employee can leave a backdoor or logic bomb that can cause disaster to the organisation (McClure, Scambray & Kurtz 2005, p.14).

In other words, organisations are at high risks. It is this human that organisation trust and give them keys in terms of passwords to ensure confidentiality of organisation's intellectual property. It is this human that organisation trust and give them authority to control data entry points to ensure the integrity of organisation's information. It this human element that organisation trust and give them privilege to monitor network traffic to prevent organisational network from system downtime. Unfortunately, it is this human element that organisation can never operate without them. Therefore, it is necessary for organisations to come up with strategies that will prevent these *"humans"* from being conned with ice-like motivations to give-up their trust.

2.4.2 Categories of threats

Furthering on the discussion of computer threats, Russell and Gangemi (1991, p.14) argues that computer threats comes into three categories; natural and physical, unintentional and intentional. Natural and physical threats include fire, flood, power failures and any disaster mainly for computer hardware and premises. On the other hand, unintentional threats consider awareness of perpetrator (Russell & Gangemi 1991, p.14). If user forgets to shut down the computer system when leaving the office or failed to apply software patches due to lack of knowledge is termed as awareness

issue. Lastly is the intentional category which is mainly the focus of this section because it combines all elements of the latter categories.

Intentional threats include those threats where the perpetrator is being driven by motivations. These motivations can either be monetary, revenge or popularity (Gorge 2007). Russell and Gangemi (1991, p.14) went further and subcategorises intentional threat into two categories; inside and outside threats. Inside threats generalise all threats that are perpetrated from inside the organisation while outside threats are those that originated from outside the organisation. The whole of this section will focus into discussing these two subcategories. The discussion will begin with outside threats and finalise with inside threats. Though there are exists massive types of these threats, but for the purpose of this dissertation only few relating examples will be considered.

2.4.2.1 Outside threats

Financial gain, revenge and/or the sense of being famous are among motivations that drive malicious events (Gorge 2007). Outside threats "outsiders" generalise all threats that are perpetrated from outside the organisation. There are thousands of these attacks from the former virus techniques where they were dependent on physical distribution, to the virus of today where they can automatically be perpetrated. However, all these attacks will be explained in three categories; technical, non-technical and hybrid.

- ***Technical threats***

Technology is evolving at a hitherto unimaginable speed. It has evolved from the ages of mainframe, where applications were limited to specific operations, to the era of personal computers where there are thousands of applications with different functionalities. However, as functionalities increases, complexity also increases so as the number of bugs (McGraw 2004). It is these bugs that are nest ground for attackers. Meanwhile, technical threats are those threats that perpetrated due to software security ramifications (McGraw 2004). Through software bugs *"vulnerabilities"*, attackers can exploit and initiate their attacks. These threats include viruses, worms, Trojan horse, denial of service attacks and many alike.

Though one may argue there is no need for employees to be aware on these attacks since they are self originated from software, employees' awareness is still crucial to

minimise their successfulness (NIST-SP 800 – 50 2003). Software developers need to discuss about how to go about developing secure software, while on the other hand end-users need to be reminded to run software patches.

- ***Non-technical threats***

Picking a phone and calling a helpdesk to pose as a system administrator who is away from the office and desperately ask for a login password pretending to issue a very crucial transaction, does not include any element of technicality. While technical threats take advantages of software bugs, non-technical threats take advantage of human behaviours and their trust (Contos 2007). Non-technical threats are those threats that are perpetrated by human.

However, this should not be confused with inside threats. In inside threats, malicious corrupted employees initiate attacks while non-technical attacks employees pose as vulnerability. These attacks are mainly characterised by social engineering techniques where bad guys studies employees' weaknesses and use those weaknesses to rule them to give out their passwords or any valuable information that eventually may cause a catastrophic damage to organisation (Fyffe 2008).

As it was explained, all these attacks are directly related to employees within organisations. If employees are well informed about all their importance in ensuring organisational computer security, and all possible ways of being conned to leak organisational intellectual properties, these attacks will at least be minimised. It is therefore necessary for organisations to appreciate employees' contribution in computer security and to frequently keep them informed on current computer threats.

- ***Hybrid threats***

As technology evolves, security tools and applications are becoming strong in protecting against computer threats. On the other side, attackers keep on changing their tactics to win the battle. As a result, human are left alone without proper knowledge on how to defend themselves against these attacks. Having spotted this loophole, attackers have now changed their tactics to integrate weaknesses from both ends. In other words, hybrid threats are those threats that combine both software errors and human

weaknesses to launch their attacks. These threats include scam emails, spams, phishing and many alike.

All these threats have huge negative impacts to the prosperity of organisation. As George (2007) ascertained, attackers do what they do because of motivations. These motivations can either be destructive, propaganda or revengeful. However, whichever the motivation of an attacker is, organisation suffers in one way or the other. Through these threats organisation can loose large amount of money, its reputation can be ruined through customers' distrustful toward its operations. Moreover, organisation's performance and its business opportunities are at stake. If a Trojan horse is planted into organisation's server where all sensitive information is stored, by transmitting this information to rivalries, the organisation would not be able to perform to its fullest.

2.4.2.2 Inside threats

Financial gain, revenge and/or the sense of being famous are among motivations that drive malicious events (Gorge 2007). This raises the question then, who is the attacker? By its simplicity, attacker is anybody who is attracted by the said motivations to conduct malicious events. Therefore, it is clear from these motivations that anybody can be a savage. Building on these explanations, it is therefore crucial to luminance employees in organisations. Following these motivations, trusted employees may betray their trust and practice malicious events. In fact, an insider threat is the hot topic in the security arena. Many researchers have researched about this topic (Schultz 2002; Kemp 2005; Contos 2007). While disgruntled and malicious corrupted employees fall under inside threats category (Bishop 2005),

Contos (2007) defines insiders as those employees who have administrative privileges and can use any system to intentionally violate security policies. Moreover, Schultz and Shumway (2002, p.189) defines inside threats as intentional misuse of computer systems by users who are authorized to access those systems and networks. Though it is not clearly stated from all these definitions, inside attackers extends to include ex-employees and third parties; consultants, contractors and temporary helpers (Schultz 2002; Kemp 2005; Contos 2007). Unlike outside attackers, insiders pose a big

challenge because they can legitimately pass electronic and physical security controls (Contos 2007).

The joint survey "Insider Threat Study" conducted in 2002 by United States Computer Emergency Readiness Team (US-CERT), United States Secret Service (USSS) National Threat Assessment Centre (NTAC) reveals that 86% of insiders held technical positions. In those cases, 81% of the organisations that were attacked experienced a negative financial impact as a result of insider activities. The losses ranged from a low of five hundred dollars to a high of "tens of millions of dollars." 75% of organisations experienced some impact on their business operations. 28% of organisations experienced negative impact to their reputations. The survey included forty-nine inside threats cases which were experienced between 1999 and 2002 (US-CERT 2008).

Authentication is one method of ensuring information confidentiality. Unfortunately, password mechanism is the common approach to it. The survey conducted by Stanton and colleagues (2005) on users' behaviour pertaining password management revealed that 27.9% of 1167 respondents write down their passwords to help them remember. However, this is motivated by the number of different passwords user needs to interact with a number of different systems in their daily operations. As usual, technology is there to serve human being. The emergent of automated tools such as cookies that keep track of users' password was embraced by users. Unfortunately these tools made things even easier for attackers to obtain users passwords (Stanton et al. 2005).

Though many solutions are proposed to deal with inside attackers, employees' awareness in security issues is still crucial (Russell & Gangemi 1991, p.13). However, it should also be noted that awareness of security policies and computer threats alone is not enough to tackle this problem. Security awareness programme(s) should go further to address the issues by making employees understand their contributions in the organisations and their benefits out of it. Furthermore, management should consider employees' incentives when practicing good security principles.

All these threats have large negative impacts to the prosperity of organisations. As George (2007) ascertained, attackers do what they do because of motivations. These

motivations can either be destructive, propaganda or revengeful. However, whichever the motivation of an attacker is, organisation suffers in one way or the other. Through these threats organisation can loose large amount of money, its reputation can be ruined by customers' distrustful toward its operations. Moreover, organisation's performance and its business opportunities are at stake. If a Trojan horse is planted into organisation's server where all sensitive information is stored, by transmitting this information to rivalries, the organisation would not be able to perform to its fullest.

2.5 Computer systems security controls

Attackers are good on what they do because of the incentives they are up to (Gorge 2007). Following these incentives, anyone can be motivated and act maliciously. Those guys from outside are working twenty-four-seven to fulfil their motives while, on the other hand, employees are betraying their trust and act maliciously. The danger is huge out there. Organisations are not safe from both inside and outside miscreants. It is now time for organisations to understand what they worth and initiate necessary control measures against these attacks.

Computer systems security has long evolve into a number of phases (Dhillon 1999; von Solms 2000; D'Arcy & Hovav 2007). As technology evolves, attackers also change their tactics, so as the control measures. From the age of mainframe where control measures intended to protect computer premises and resources usage, to the client-server era where single access controls were appropriate control measures, up to web services arena where there is a need of international standards and highly expertise in computer security. Many researchers contributed in describing this evolution (Dhillon 1999; von Solms 2000; D'Arcy & Hovav 2007).

Dhillon (1999) describes computer security based on three intervention; technical, formal and informal. He explained the reliance of technology like message authentication, encryption and digital signature (technical interventions), and emphasised on organisation restructuring to accommodate computer security (formal interventions). In informal interventions he emphasised on the importance of educating users in computer security issues.

von Solms (2000) describes computer systems security into series of waves. In the first wave he described computer security based on technical controls like user passwords and ids. In the second wave he focused on management involvement in computer security where he mentioned the establishment of security policies and procedures. In the final phase he focused on the need of international security standards and security certification, organisational security culture and keeping an eye on control measures.

Moreover, D'Arcy and Hovav (2007) describe computer security with four countermeasures; security policies, security awareness programs, computer monitoring, and preventive security software. The first and second countermeasures emphasises on enforcing security good conducts by defining security requirements in terms of users' responsibilities and procedures, and inform their duties and consequences of their ignorance. Computer monitoring provides a close watch of users' behaviours whereas the last countermeasure focuses on protecting against unauthorised access.

All the above analysis of computer security share common perceptions. Almost all descriptions explicitly, if not implicitly, explain technical, management and institutional security control measures. Therefore, in order to be consistent, this section will adopt the approach described by von Solms (2000) to describe different computer security control measures. This approach was chosen because it reflects the reality of implementing security control measures based on organisations' needs. The summary of what constitute in each phase is provided in figure 3.

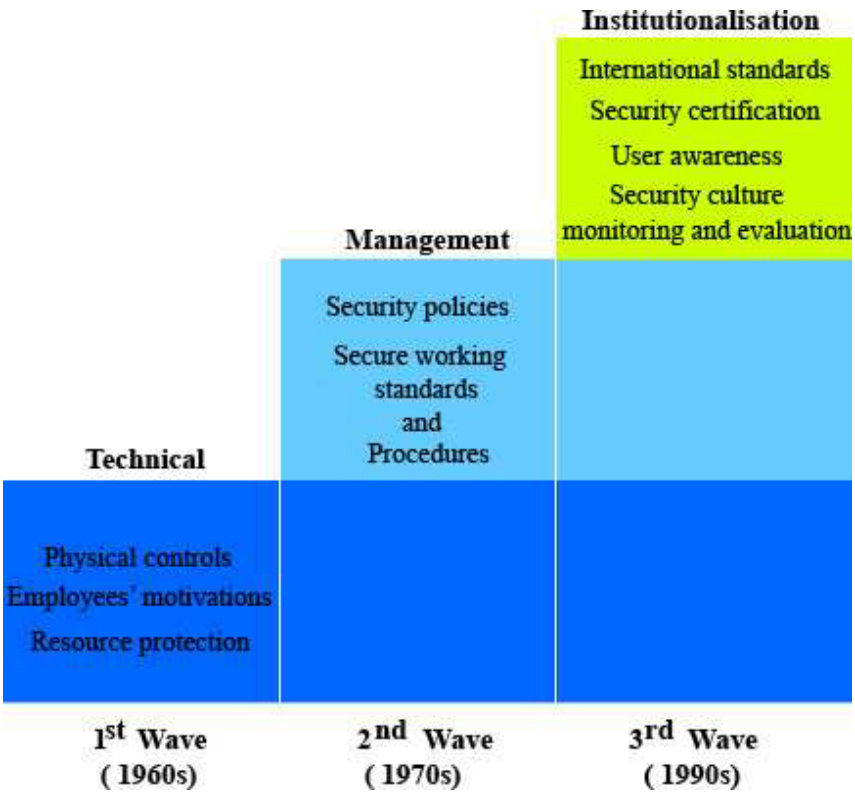

Figure 3: Summary of security control waves

To begin with the discussion, this section starts by the discussion of first wave where it includes the discussion of all physical and technical security control measures. The discussion of the second wave will follow where all managerial participation in computer security will be discussed. Finally, the discussion of the third wave where it will describe international security concerns and the focus of human factor in security controls. In this section each phase will be used as an umbrella to accommodate all security control measures that fall under that category.

2.5.1 The First Wave - Technical

Computer threats are evolving with technology evolution. The more technology introduce us new magic, the more attackers are closing the gap toward us. Technology in its embryonic stage, computer attacks required physical mechanisms like floppy disks for virus distribution or physical tapping of cooperate network. However, things are different now. With an openness of internet, attackers are able to launch there attacks almost anywhere in the world. Only your IP address is enough to track where

you are. Although there are voluminous of control measures to deal with these attacks, this section will only explain some of them.

Technology in its dawn, computer security was not a headache. This was the time when physical guiding of computer rooms was enough to ensure safety of computer system and its resources. In this era, security related roles concentrated on physical controls and suitable motivations for computer operators (Janczewski & Colarik 2005, pp.6-7). Their main concerns were limited to power fluctuations and natural disasters like fire and flood. This was the time when identification cards, fire alarms, sprinkler systems, temperature gauges and surge protectors were enough for computer security (Russell & Gangemi 1991, p.14).

Furthermore, to control computer system from unauthorised access, operating systems' facilities like account access controls, user ids and passwords were enough to guarantee the security of organisation's information resources (von Solms 2000). However, this unauthorised access meant protecting the system from computer resources abuse (Andress 2003, p.1). This was the time when computer memory and speed were scarce resources.

As computer memory and speed increased, and after organisations' realisation of the power of information, computer controls shifted to enhance confidentiality and integrity of information (von Solms 2000). In their initial forms, these controls focused on prevention of information disclosure by limiting illegal copies of information stored on magnetic media or hard documents (Janczewski & Colarik 2005, pp.6-7). Things changed when information sharing arouse. More technologies such as granular access control, single sign-on and encryption were developed to prevent unauthorized access and modification (Andress 2003, p.1).

However, with all these control measures the number of computer break-ins kept on increasing. The complexity of software applications kept on increasing, so as the number of bugs. Moreover, software engineering paradigm did not consider the issue of security as their concerns. On the other hand, users who operate computer systems and the so called security tools and applications were left unaware of the current computer threats and how they attack.

2.5.2 The Second Wave – Management

As it was mentioned previously, computer security is a three magnitude process. It involves technology, people and process (Andress 2003, p.5). Failure of one component leads to the failure of the whole process and hence leaves the organisation and its sensitive information in a jangle. The first wave of computer control measures, organisations strive to acquire the most sophisticated technologies to patch security holes. Security controls ranged from physical controls where the focus was on protecting computer premises, to the installation of necessary technologies to combat with computer attacks.

However, as technology kept on advancing, information became an organisational asset hence management involvement in computer security became apparent (von Solms 2000). This was the time when organisational security exceeded its boundaries by maintaining organisation's reputation by considering costumers' trust and satisfaction (Herold 2005, pp.7-14). Technical personnel realised the pressure of maintaining corporate security and they demanded for power to control corporate security. This was when security policies were introduced in organisations to enforce employees' accountability for security related activities (Herold 2005, p.15).

The first initiative to establish security policies was by US Department of Defence (DoD) in 1970s where they sponsored a research which focused on developing security policy models (Russell & Gangemi 1991, p.30). The first form of security policies was simple only concentrating on guiding employees from drinking or smoking in computer room (Russell & Gangemi 1991, p.14). However, as technology evolves new policies are emerged to cope with current security issues. Security policies for guiding employees from smoking or drinking do not work with today's technological advancement. Internet, World Wide Web and the so called E-commerce demands more sophisticated policies on ensuring online trust and internet usage within organisations.

However, all these security policies are not enough to ensure maximum computer security within the organisation. The worst part of is the nature of policy establishment. Policies are established based on computer threats. Therefore with this growing nature of technology, it is apparent that there will be thousands of policies to

be followed. Moreover, it is nearly impossible for these policies to luminance every aspect of human concerning with computer security. Technology is unpredictable parameter therefore organisations should focus more on building their manpower to exercise computer security ethics. Management should show their concerns with computer security, and the potentiality of its subordinates in ensuring corporate computer security.

2.5.3 The Third Wave - Institutionalisation

As technology advances the world becomes a single village. The issue of computer security become a global problem. Physical and technical controls and ordinary organisational security policies become out weighted when it comes to digital world. This is the era that characterised by computer security standardisation, international computer security certifications, security culture and dynamic measure of computer security control measures (von Solms 2000). In this wave, computer security control measures shifted from organisational interests to governmental and international interests. The interest is not how the organisation benefits from computer security, but what organisations do to ensure customers' privacy and state security.

In this wave the focus is the state level of information and computer security management and combination of experiences of several big organisations in computer security management to form a consensus on common international information and computer security standards (von Solms 2000). This can be exemplified by European Data Protection Directive that focuses on privacy protection of citizens by insisting training to employees about privacy issues. However, this is directive focus only within European Union. On the other hand, Sarbanes-Oxley (SOX) Act focuses on controlling financial activities.

In this wave, management shifted their gears to consider training and education to its employees. The locus shifted from just maintaining corporate information to the compliance of the growing number of laws and regulations that enforce information protection and customers' privacy (Herold 2005, p.5). Moreover, the international image of computer security is reflected with the existence of pool of security qualification certificates. Following ISO standards which also emphasises on

employees' training, there are security qualification certificates that focuses on equipping information security personnel with appropriate skills to initiate and execute training programme in organisations.

2.6 Conclusion

This chapter aimed at investigating current situations on computer threats as associated with users and the efforts organisations undertake to control them. In computer systems background, a discussion of computer evolution in relation to computer security was conducted. In this chapter, it is pointed out that the advancement nature of technology has a large impact on computer security by both introducing more bugs into applications and attracting more users who are most susceptible to computer threats. Moreover, it is this technology that facilitates the advancement of computer attacks by offering more convenient ways for attackers to launch their attacks.

Moreover, in this chapter human element has been identified as a central to successfulness of computer security and organisation's prosperity as well. It is human element that is responsible to maintain confidentiality, integrity and availability of organisation's information resources. This view directly correlates with the increase number of inside threats. Employees are either unintentionally or intentionally ignore organisation's security requirements and hence encourages more security break-ins which results to loss of reputation, competitive advantages and money to the organisation.

Many computer security control measures have been implemented, from technical through managerial to institutional, to combat with computer threats. Unfortunately, with all these efforts the number of computer threats keeps on increasing. Although among these control measures security user awareness has been identified as the key to successful computer security, it either receives little emphasise from management or lacks appropriate approaches to attract users' participation. Therefore, the next chapter provides the discussion of security awareness with emphasise on investigating users' involvement in security awareness and the effectiveness of current security awareness programmes in educating users.

3 SECURITY AWARENESS

3.1 Introduction

As it was explained previously, many security mechanisms exist to fight against the current computer threats. Although there is recognition that the human factor plays an important part of security mechanisms, the role of user awareness receives limited attention. Security user awareness programmes focus at informing users on their roles and responsibilities and imparting them with appropriate knowledge to fulfil them. However this should not be confused to end-users alone. Managers' and IS specialists' involvement should also be taken into considerations. Currently, there are many types of security awareness programmes but they overlook the importance of users' involvement in security awareness material preparation.

Although security awareness is just one component of security learning circle, for the purpose of this dissertation it will be discussed in detail with other components being presented in less detail. The main aim of this dissertation is to develop a framework to harness the power of KMS to improve security awareness. However, it is worth to have a clear understanding of security awareness in an organisational context and identify key issues that have been notified in literature as crucial for successful implementation of security awareness programme(s).

Due to the influence of security awareness in information systems' security, much has been written emphasising its different aspects. However, in this dissertation, the focus will be only be on exploring different perceptions of security awareness programme, designing process, current awareness programmes, their success and failure and security awareness in developed and developing countries. Though developed and developing countries includes many countries, this chapter will only consider Ireland and Tanzania as developed and developing countries respectively. This chapter concludes by outlining the crucial bits for the success of security awareness programme(s).

3.2 What is security awareness?

In chapter 2, many security threats and their possible solutions have been discussed. The majority, if not all, of these threats are either caused or driven by human element from both top managers and operational employees. Software flaws, caused by developing team, are very common in this era of project *deadlines*. They are very common gateways for security threats. On the other hand, *social engineering* dominates in ruling employees into opening gates for attackers. It is therefore very crucial for organisations to take into account users' education in security relevant issues.

As it was explained previously, security is a three magnitude process. It involves technology, people and process. This implies failure to one component results to the failure of the whole process (Andress 2003, p.5). There is no doubt on the maturity of technological security controls. The existence of anti-virus, anti-spam, firewalls, network sniffers and many alike all, shows the extent to which technology has dominated computer security. However, user' education on security relevant issues receives a minimum attention. As a result many security awareness programmes fails. This section explores what exactly a security awareness programme is, the roles that must be involved and its differences from training and education.

3.2.1 Security awareness - Defined

Prior to delving into discussing security awareness programme, it is worthwhile explaining the differences between security policies, security awareness and security awareness programme. Russell and Gangemi (1991, p.30) defines security policy as a tool for enforcing computer security by declaring rules, standards and regulations on how computer and information assets should be managed within an organisation. On the other hand, Desman (2002, pp.3-10) defines security awareness as employees' understanding on security control measures and their consequences. The former defines security requirements while the latter determines users' understanding. Furthermore, NIST-SP 800 – 50 (2003) defines security awareness programme as the vehicle for disseminating information that users need in order to do their jobs. It is then clear from the definition that the latter communicates security requirements.

However, there is still a conflict on what exactly is security awareness programme. As NIST-SP 800 – 50 (2003) defines, security awareness programme as a vehicle for disseminating information that users, including managers, need in order to do their jobs. On the other side, Nosworthy (2000) defines security awareness programme as a tool to impart users with appropriate knowledge to perform their duties. The former definition emphasises on informing users about what they should do to ensure security of corporate information assets and the consequences of their security related decisions. Contrary, the latter definition emphasises on imparting users with appropriate knowledge to perform security related responsibilities.

The former definition lacks the reflection that it should also be a tool to impart users with appropriate knowledge to perform their duties (Nosworthy 2000). How can a user know how to deal with new phishing techniques without being imparted with appropriate knowledge? The awareness of roles and responsibilities must go hand-in-hand with appropriate knowledge so as to enable users to participate in improving organisational security. The latter definition can also be backed-up by the work of D'Arcy and Hovav (2007) where they defines security awareness programme as the improvement of users' understanding on their responsibilities on ensuring security of organisational knowledge and information resources, and the consequence of ignoring or abusing these resources by imparting them with appropriate skills to fulfil their responsibilities.

Therefore, throughout this dissertation, security awareness programme will be regarded as a twofold role. The first role *"awareness"* as a means of disseminating information about users' responsibilities, working standards and procedures (Desman 2002, pp.3-10) and the second role *"simple training"* as disseminating security relevant material explaining current issues of computer threats so as to combat users with appropriate knowledge to fight against these threats (D'Arcy & Hovav 2007). However, it is worthwhile explaining *what*, *who* and *how* parts of security awareness programme. The "*what"* part explains what should be disseminating, "*who"* explains the target audience and *"how"* explains the procedures for accomplishing the *"what"*.

Consider this scenario. Security personnel of organisation "A" drew a policy to strengthen employees' passwords. The policy only states the minimum requirement for

password length as 14 characters long. What do you think will happen to employees? Will they ignore the policy for the fear that the password will be too long? The answer is obvious no. Users tend to go for a cheaper solution, they will comply with the policy by creating a 14 long password but only with letters, which is easy to be hacked. Therefore, without imparting users with appropriate knowledge on how to create strong passwords they can still adhere with the policy but in their simplest way which creates a burden to computer security. This concludes that the *"what"* and *"how"* of security awareness programme should go hand-to-hand.

Who are target audience? This question is the same as whose are security policies for? As it was defined previously, security policy is a tool for enforcing computer security by declaring rules, standards and regulations on how computer and information assets should be managed within an organisation (Russell & Gangemi 1991, p.30). This implies that the issue of computer security is an organisational issue, therefore there is no exceptional. Since security awareness programme is a tool for selling security policies and relevant security issues organisational wide therefore all levels of organisational management must be included (NIST-SP 800 – 50 2003).

3.2.2 Relationship between security awareness, training and education

Security awareness is just one component of organisational security learning process (NIST-SP 800 – 50 2003; Microsoft 2006). The cycle, as described in later sections, consists of three components; awareness, training and education. However, there is confusion on what constitutes awareness, training and education. Therefore, it is worthwhile to bring their differences in this section so as to have a clear picture of their meaning and purpose.

As it was previously defined, security awareness is the understanding of security controls and their effects on organisational IS security (Desman 2002, pp.3-10). Moreover, D'Arcy and Hovac (2007) and Microsoft (2006) explain the purpose of security awareness as to change users' behaviour by combating them with appropriate security knowledge. On the other hand, training as Microsoft (2006) and NIST-SP 50 (2006) explains, its main purpose is to impart users with new computer security skills. However, it should be noted that the training that is being considered here is absolutely

different with the "simple training" as mentioned previously. This one is more formal while the former is highly volatile, changes with the daily needs of security requirements.

In short, awareness focus on changing employees' behaviour on specific security issues while training focuses on giving new skills to perform a specific function (NIST-SP 800 - 50, 2003). Awareness targets everyone in the organisation while training only focuses on group of people especially technical staff. Education, on the other hand, focuses on creating new knowledge and skills about computer security in a broader view by considering other fields like psychology, philosophy and many others (Buckley & Caple 2007, p.6). This level is mainly for security experts who wish to expand their security knowledge and relate with other disciplines. More distinctions of these three components can be obtained in table 2.

	AWARENESS	TRAINING	EDUCATION
Attribute	"What"	"How"	"Why"
Level	Information	Knowledge	Insight
Learning objectives	Recognition and retention	Skill	Understanding
Example Teaching Media	Media (Video, Newsletters, Posters)	Practical Instruction (Lecture and/or demo, Case study, Hands-on practice)	Theoretical Instructions (Seminar and discussion, Reading and Study, Research)
Test Measure	True/False Multiple choice (identifying learning)	Problem solving i.e. recognition and resolution (apply learning)	Essay (interpret learning)
Impact timeframe	Short-term	Intermediate	Long-term

Table 2: Awareness, Training and Education - Comparative Framework

(Source: NIST-SP 800-16 1998)

3.3 Security awareness building process

As was mentioned previously, security awareness programme is the focal point for practicing good security principles. If it is well executed, security awareness alone is

enough to recover organisation from the hands of attackers (NIST-SP 800 - 50 2003). It plays a very difficult role of transforming human behaviours into embracing security principles. Therefore, understanding its building blocks is a one step for the development of an effective framework to support security awareness which is an aim of the project in this dissertation.

Much has been written about the development of security awareness. However only the approach proposed by Desman (2002) will be considered in this dissertation. This approach was preferred because it is a generic approach; there is no an element of biasness due to organisation or country. Desman (2002) describes the process of building information security awareness programme(s) as being divided into four phases: getting started, establishing baseline, communication and evaluation. In this dissertation, the approach is termed as generic approach. However, it should also be noted that this name is only for the purpose of this dissertation and not otherwise.

3.3.1 Getting started

Desman (2002), argues that understanding organisational culture is the key to the successful of security awareness programme(s). He commented that by doing so it will help in understanding management team, the “do’s” and “don’ts” of the organisation and the current workable communication channels in the organisation. Moreover, he also suggested that one must ferret for available resources that are useful for a successful accomplishment of the programme. These resources includes any control measure documentation and any communication channels that are available.

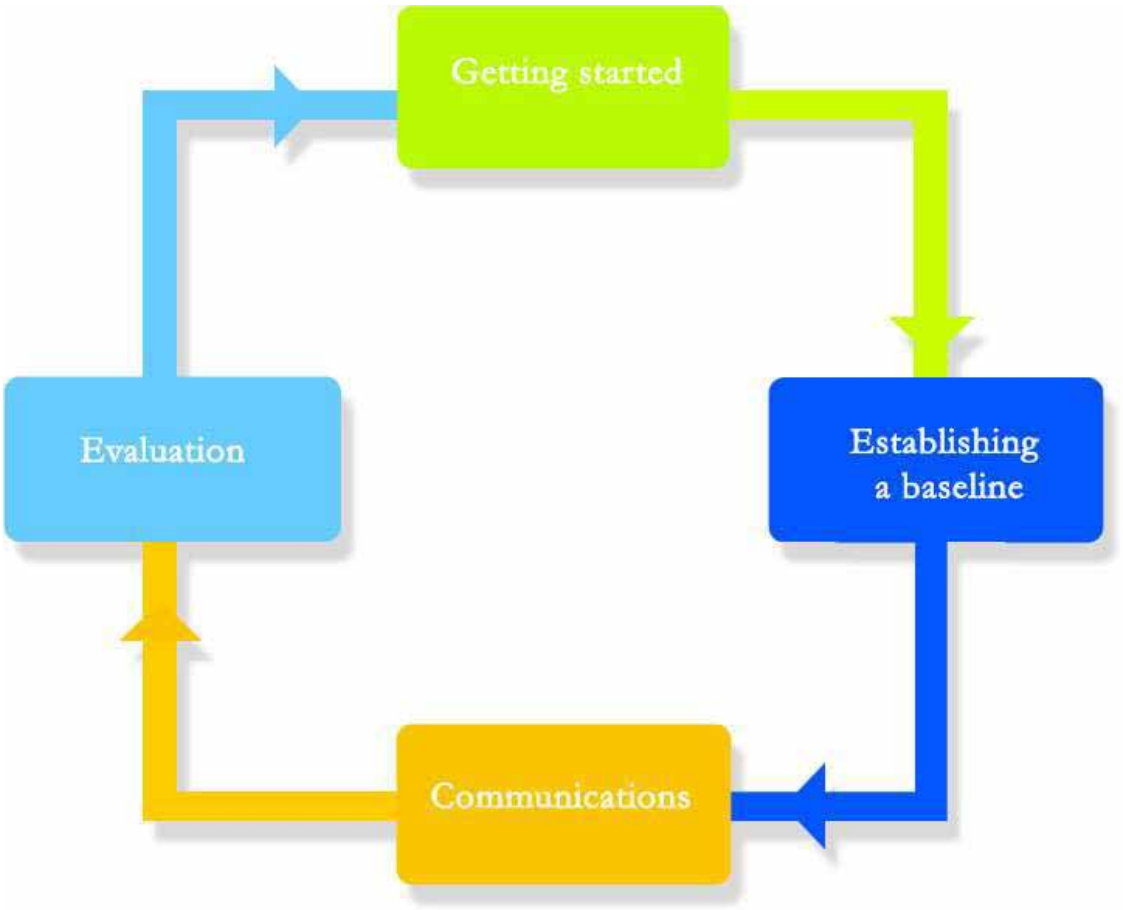

Figure 4: The process for building security awareness programme

3.3.2 Establishing a Baseline

"Building on giant's shoulders." is a common axiom that we use. After rummaging for existing resources to use, understanding organisation's key personnel and understanding its culture, now it is time to sit down and decide what is to be excluded or included in awareness programme and with what extent of amendments. Many of obtained control measures might be outdated. Therefore, one need to evaluate the necessity of these control measures by reflecting the current situation and decide to whether replace them or make them endeavours prior to documentation (Desman 2002).

Desman also emphasised on the involvement of users who in one way or the other participated in the creation of control measures at hand, and also the necessity of wining users' commitments. However, his main concerns were focusing on "big guys" who set control measures. The question is what about those people who have not

participated in creation but yet they are affected with these control measures? This is in fact a very crucial point to miss. Users, at all level, should be consulted for their contribution on what seems for them to be necessary for the assurance of corporate computer security.

3.3.3 Communication

After all necessary procedures to create security awareness materials and that the document is already set, what follows then is to get the prepared materials reach all people in the organisation. Desman suggests a number of methods to fulfil this task including video taping, PC programs, email and web pages and finally paper-and-ink approach. In PC programs he explained about moderated screen show with facilitator presenting the document and its contents, self-paced moderated screen show and on terminal video show. In the latter method he suggested on screen pop up of the show. This is when a user login to his/her accounts and receives an option to watch the show or ignore it.

In fact the approach of making users watch the scene about security concerns whenever they login is an effective approach because it gives them everyday updates on security status. Therefore, if there is a new security break-in, this approach is useful to deliver the information to users in a real time. One major problem which Desman notifies is the awareness of employees who are in holiday. However, this approach is even useful when they come back or even when new employees join the organisation. Though this may sound to be much involving in respect to time required to sit down and watch the movie, a little adjustment of the contents might turn the coin “face-up”

3.3.4 Evaluation

All the way from rummaging for existing control measures and communications media, amendments and replacements of security controls up to letting the word out, letting users to know what has been done, it is a long journey to be left out without monitoring its progress. Desman encourages monitoring and evaluation of the program so as to evaluate its progress, or otherwise. The aim of the program is to educate users on their roles in computer security and the consequences of their ignorance toward computer security.

Desman (2002) proposes two approaches for monitoring and evaluating security awareness programme; number of break-ins and audit reports. *Number of break-ins* focus on pre and post evaluation of computer threats. This type of evaluation can take any form; interview or questionnaire. The common questions are like, did the number of break-ins increased since the introduction of awareness program? If yes, then what could be wrong; the materials covered are irrelevant or they have not reached users at large? Moreover, useful information can be obtained from *audit trails*. The number of password failure attempts, attempts to delete system files and may alike. Whatever findings from the evaluation, could be very useful information to act as an input for the next security awareness materials

This approach is useful because it considers almost every angle of successful building of security awareness programme. As it was mentioned in getting started, emphasise should be put on understanding organisational culture. Culture is a strong element for major changes, so by taking it into account, it means that security awareness programme is in the right track for its successful implementation. Moreover, it is also important to consider people who participated in the development of previous control measures since they may provide some useful information for the successfully accomplishment of the programme.

Moreover, a crucial bit of successful security awareness programme is the means of communication to deliver what has been prepared to users. Security policies and relevant materials should reach employees within organisation at large. Therefore it is necessary to opt for communication channel that is acceptable by the people who use it. Failure to do so may result to ignorance and hence failure of the programme. Finally, there must be some sort of evaluation of the programme. Despite the cost spent during programme development, awareness programme aim at reducing the number of break-ins by equipping employees with appropriate knowledge. Therefore, it is plausible to evaluate its successfulness or otherwise.

However, the question then arouse, is this security awareness programme that we are talking about tackling the current state of computer threats where threats evolve at an alarming speed or for a long-term plan? If it is for daily, more dynamic environment

then this approach is obsolete, unless stated clear that all these steps are for building permanent long-term security awareness programme that will be evolving with the change in environment.

3.4 Current security awareness approaches

The journey to implement a successful security awareness programme is a long journey. Understanding the *"what"*, *"who"* and *"how"* part of it, is just one step for its implementation. As it was previously mentioned, much must be covered prior to actual implementation of security awareness programme. Desman (2002), describes the implementation process with four phases of which each has several subsection that explains mosaic of factors to be covered. Since designing a framework for security awareness is the aim of this dissertation, it is worthwhile to explore how the olds have played the game so that we can snatch some tips out of them.

This section will explore different approaches of security awareness programme by examining the applicability of the above defined implementation phases. Though there are mosaic of security awareness approaches, this section will only focus on five categories that are mostly deployed in industry; incorporating in employment agreement, face-to-face, awareness tools, awareness games and web-based. The section will finalise by identifying common weaknesses as spotted in these approaches. To begin with, the discussion of incorporating security awareness in employment agreement will be provided then followed by the discussion of face-to-face approach. Thereafter the discussion of awareness tools and games will be provided and finalise with the discussion of web-based approaches.

3.4.1 Security awareness in employment agreements

Security awareness programme can take many forms. It can be delivered as a game based, face-to-face, awareness tools, web-based. Herold (2005, p.40) proposes an approach of incorporating computer security requirements into job descriptions, employment agreements and awareness acknowledgements. It is Herold's idea that by incorporating security awareness in employees' recruitment processes it increases the accessibility of security awareness materials since each employee follows the same channel of recruitment.

However, this approach is more static and focuses much on disseminating of security policies. The world of digital threats is moving fast. If we need to be safe, then we need a more dynamic and real time security awareness approaches. It is insufficient for users to just be aware of their responsibilities and the impacts of their decisions. What is sufficient is to induce security mindset by making computer security as our daily conversations.

3.4.2 Face-to-face security awareness programme

There are many approaches of face-to-face security awareness programmes (Schifreen 2006). These approaches range from personal-based to group-based security awareness programmes. Personal-based approaches are when a trainer focuses only with an individual employee, while group based is when the trainer focuses on a number of users. Schifreen (2006, p.56) and Herold (2006, p.225) argues that in-personal awareness training is appropriate approach because it reduces interactions between audiences and hence increases their attention.

However, the applicability of what has been presented during the awareness session depends on the availability of summary material of what has been discussed (Nosworthy 2000). They need a good reference material to refer what has been discussed. If reference material has been prepared such that it can be used on a daily basis then employees would be encouraged even more to use what they have learned (Nosworthy 2000). Moreover, the effectiveness of this approach relies on the instructor. Most organisations take expert from the domain to conduct a presentation. However, being expert not necessarily good presenter (Herold 2005, p.56).

3.4.3 Security awareness tools

As an effort to overcome computer threats based on software vulnerabilities, Sankarpandian and colleagues (2008) developed a tool that triggers users' awareness about un-patched software in their system by painting graffiti image on users' desktop, see figure 5. TALC which stands for Threat Awareness, Learning, and Control, constantly searches for any installed software in users' machine then compare the results with predefined list of software with available patches from NIST National Vulnerability Database (NVD) (Sankarpandian, Little & Edwards 2008).

Figure 5: Screenshot of TALC Anti-Phishing Tool

(Source: (http://www.cc.gatech.edu/))

If it finds a new patch, it verifies if it has already been applied in corresponding software that is currently installed in user's machine. If it has not been applied, the tool draws a graffiti image to notify user about a threat, see figure 5. When user's cursor hover over graffiti area, the tool displays the name of that software and the type of threat it might cause. This is done by consulting NVD at connection time to retrieve patch information. Threat severity is indicated the size of graffiti image; the larger the image the higher the severity.

Although TALC was developed to specifically help home users against computer threats based on software vulnerabilities, but it can also effectively work in organisation environment where there is no centralised patching system like Marimba Patch Management (http://www.bmc.com). However, to effectively handle cross-cut computer threats, the tool need to be upgraded to accommodate other threats like phishing, social engineering, spam emails, password management any many alike.

3.4.4 Security awareness games

Participatory approach is among new teaching technique that is being practiced in academic institutions. It is a very effective method because it draws learner's attention throughout the session. Since it's a teaching approach, there is no exemption for its applicability into imparting users with appropriate knowledge to deal with different computer threats. In this approach users participate into identifying attackers' malicious events by playing game.

After realising the power of games into delivering knowledge, Sheng and colleagues (2007), designed an anti-phishing game that focuses on imparting users with knowledge to detect malicious websites, see figure 6. They obtained a list of phishing URLs and categorised into three categories where training messages were created for each category. These messages were then embedded in the game as help and feedback explaining what should be and/or have been done respectively (Sheng et al. 2007).

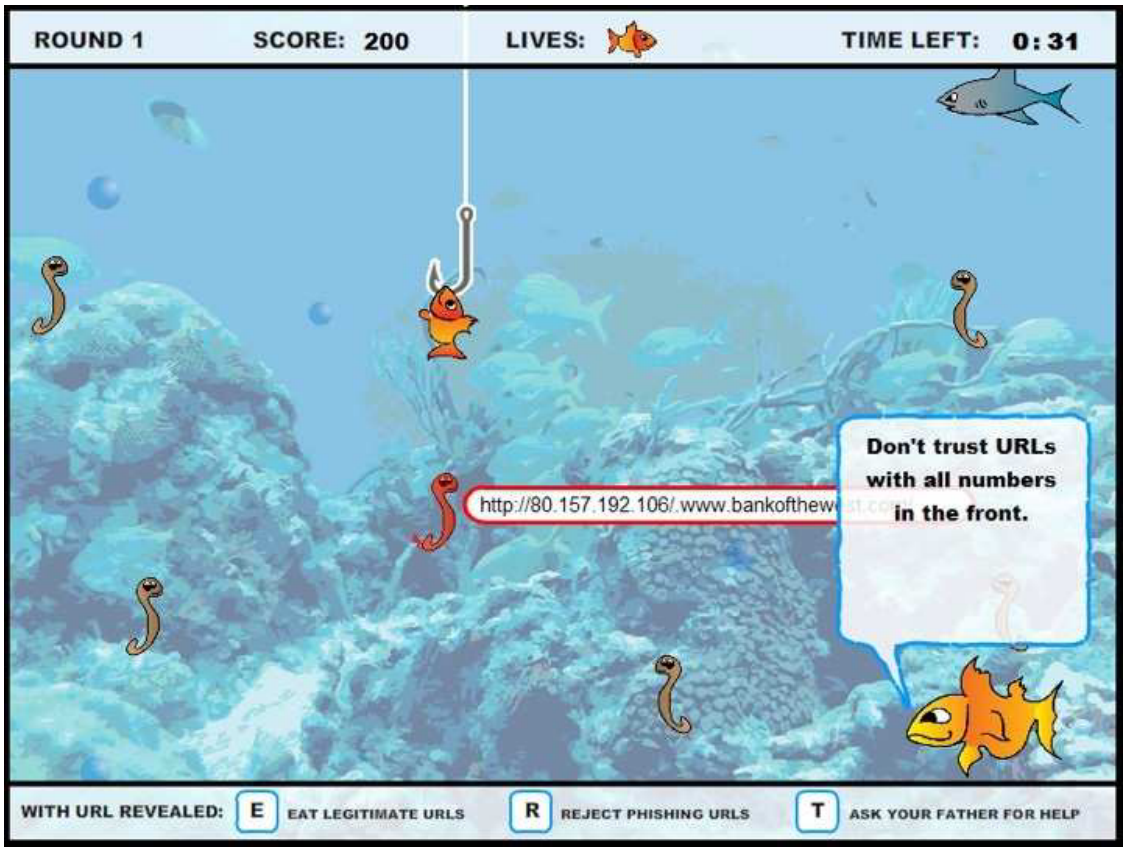

Figure 6: Screenshot of Anti- Phishing Phil Game

(Source: (http://www.cmu.edu/))

However, the approached is too narrow focusing only on Web sites' URLs. Suppose, in real world, user failed to identify the phishing URL, what should other tips user go for? This approach only equips users with phishing websites identification and ignored other side of the coin. Moreover, the approach is too rigid; too stiff to include other computer threats. The approach need to be very flexible to accommodate any computer threat at hand (Sankarpandian, Little & Edwards 2008).

3.4.5 Web-based approaches

Face-to-face security awareness approach is inappropriate when the organisation is of mega size. To conduct security awareness programme in an environment like this it involves both time and money. Therefore, in the environment like this a web-based approach can be deployed. The common methodologies in web-based approach are security awareness via e-mail and organisational websites. E-mail approach is when security personnel posts security related updates to employees through organisational or personal email accounts. On the other hand, website is also being used to post security related issues.

However, both these approaches have limitations; they only provide a one way communications. Though web technology offers much functionality that can effectively facilitate security awareness, majority of current web-based awareness programmes ignores these functionalities.

Incorporation of security awareness in employment agreements, face-to-face, security awareness tools and games, and web-based approaches, all these have limitations on effectively communicating security related issues to employees. Their rigidity nature and poor accessibility of employees both reflects their ignorance of security awareness building process. Having security awareness programme in place without a proper employees' change management could lead to ignorance of the programme and hence failure of security awareness programme. Therefore, to be successful, we need to involve employees from initial stages of building process so as to build collaborative nature between security personnel and end-users.

3.5 Security awareness in Ireland

"Minister launches internet security awareness campaign" the opening headline of the Ireland's national news independent website, http://www.independent.ie, on February 11, 2008. It is not the intent of this section to relay news about security awareness, but the headline reflects the efforts of which the government of Ireland has taken into fighting against computer threats. Although there is no scholarly literature that have specifically discussed about security awareness in Ireland, but with this piece of information, it is clearly that the issue of computer security has flooded from organisations to the public concerns.

Although the aim of this dissertation is to develop a framework to leverage KMS to improve security awareness, it is crucial to understand how different countries perceive on security awareness. The intent is to develop an open framework that can be applied elsewhere in the world; therefore it is worthwhile investigating how different countries perceive the issues of security awareness. Ireland was chosen because it was within the reach of the author and it also represents developed countries.

Irish government has initiated many campaigns to increase public awareness on computer security matters. These campaigns involve different categories of audiences including children who are tomorrow's generation. However, due to lack of source of information, this section will only concentrate on web-based security awareness approaches specifically to websites and blogs.

3.5.1 National campaign on security awareness

Understanding the benefits of computer systems and its applications, and the danger that exists on internet services, the Minister for Communications, Marine and Natural resources launched an official website as a central for National Awareness campaign on Computer security (http://www.ncte.ie). http://www.ncte.ie is an open website which aims at providing free tips on computer security to different users. Among the users are business, citizens, legal and kids.

This is powerful strategy to motivate both individual and organisations to leverage computer security issues in their daily operations. However, the campaign overlooked

the involvement of computer and security experts. It overlooked the fact that even security experts need to be considered in the periodic education on security matters. The website focuses mainly with end-users from different sectors.

3.5.2 National Centre for Technology in Education

The National Centre for Technology in Education (NCTE) is an Irish Government agency established to provide advice, support and information on the use of information and communications technology (ICT) in education. Following the same strategy of raising security awareness within Irish community, NCTE had gone further by providing security awareness to its audience under an open website *webwise* (http://www.webwise.ie). This website provides security awareness on different topics in computer security.

The website provides awareness into three categories of audiences; children, teens and adults. One of the strongest features of http://www.webwise.ie is the ability to deliver the message based on the category of audiences. For instance, for kids it uses cartoons to elaborate security relevant issues. Moreover, to delivery teens' security matters, http://www.webwise.ie connects to another open website watchyourspace.ie where teens can obtain security issues based on the scenario that suits them (http://www.watchyourspace.ie). http://www.webwise.ie also provides video clips and *"how to"* link which elaborates security issues.

3.5.3 Internet Advisory Board

The Internet Advisory Board (IAB) is an Irish body which is responsible on assisting and supporting the Irish Internet Service Provider (ISPAI) industry to deliver an effective self-regulatory environment for internet content (http://www.iab.ie/). Apart from its core duties, IAB also promote awareness of internet safety, particularly with regard to children.

It provides guiding information to parents on different techno-social aspects concerning their kids. Although, in one side, it is a weakness to only concentrate to parents and ignores other categories of users, but in the long run its results could be

tremendously. This is because good ethics that are being taught to kids grows with them and these kids, in some days, may turn to be good computer security generation.

Ireland is far ahead in security awareness campaign. Government has initiated many security awareness initiatives which if they will be maintained and periodically improved, Ireland will be the leading territory in Europe in computer security ethics. Irish government has shown a good example that can be adopted with other countries. Its strategy to educate children in a secure way of using internet and computer systems in general, it is a strongest strategy that prepares the next generation to be security savvy. It makes children to grow with security mindsets and eventually computer security will be adopted in society.

3.6 Security awareness in Tanzania

"Currently very few educational institutions have computer laboratories..." and *"Tanzania needs to create and sustain a secure cyber-law environment..."* are the two statements that are enough to reflect the perception of security awareness in Tanzania (http://www.tanzania.go.tz). Tanzania, like majority of African countries, it is very far behind technology, so as computer security. Tanzania was chosen in this dissertation because it was within the reach of the author and it also represents developing countries.

The evidence shows developing countries are far behind computer security (Cole et al. 2008). There is no a central body for establishing legal actions on both computer abuse and Cybercrime. Currently organisations rely on their security policies as the means of protecting their information resources (Bugada 2005). On the other hand individuals with internet access at their homeplace relies on Internet Service Providers (ISPs) to provide them with some sort of security, only with the exceptional of few home users with antivirus applications.

Therefore much effort is required in organisations that are in developing countries. Executives need to be educated on the danger of corporate information assets so as they can be willing to fund security control measures and also motivate its employees' participation in security issues. However, though this can be seen as a big challenge in

computer security context, still it can be advantageous to researchers to develop a model that can be used by developing countries when deploying new technology.

3.7 Failure of current security awareness-findings

Based on the conducted intensive literature review on both computer security and security awareness, it is clear that the successfulness of security awareness programmes goes with four essential parameters; programme material, mode of delivery, security culture and organisation culture. Failure to comply with these parameters leads to failure in successful execution of security awareness programme.

The former parameter concentrates on the content that needs to be delivered to the targeted users, while *mode of delivery* focuses on the means of disseminating security awareness material. *Security culture* focuses on motivations and initiatives toward computer security, while *organisational culture* focuses on the "don'ts" and "do's" of the organisation. Though there are many scenarios to elaborate these parameters, this section will only concentrates on major ones.

3.7.1 Material delivered to audiences

It is boring when attending a chemical engineering presentation of a professor who frequently uses chemical terminologies while you are not from that domain. However, it is enjoyable listening to Knowledge Management module because you are familiar with the terminologies. Unfortunately, the same case happens in security awareness programmes. Many organisations overlook the *need assessment* of security awareness materials and instead they buy on shelves material and without even customising to meet the nature of organisation's problem (Herold 2005, p.56). This not only makes security awareness session boring but also ruined organisational computer security.

3.7.2 Mode of material delivery

Mode of delivery is another crucial parameter. This concentrates on how security policies and security relevant materials are being conveyed to employees. Security relevant material should be channelled through the media that is accepted by both ends of organisational chart; from top management to operational personnel (Desman 2002, pp.19-26). However, this is an organisational culture issue; what are the doable and

undoable. Mode of security policy and awareness material delivery must be effective enough to both gain high accessibility to organisation as a whole and to be in real time.

3.7.3 Organisational security culture

Current security initiatives and users' motivations have impact to the successful embracement of security awareness programme within an organisation (Chia, Maynard & Ruighaver 2002; Herold 2005, p.35). Many researchers have talked about organisational security culture but to author's knowledge none have tried to define what it is (Chia, Maynard & Ruighaver 2002). Therefore, for the purpose of this dissertation, organisational security culture can be defined as an organisational subculture that focuses specifically with security relevance initiatives and motivations. This is mainly under the Computer Systems and Information Security department. However, this must correlates with the nature organisational culture.

There is no direct tangible benefit of security to users (Bishop 2005, p.16). If there is nothing in return, security will turn to be an option to users. However, though there might be security policies to bind users to do and not to things, users tend to ignore these policies. For instance, though many organisations have "do not share your password" policies, survey revealed 23% of 1167 respondents share their passwords with their colleagues within and outside their working places (Stanton et al. 2005). These passwords may result to financial and/or information theft, loss of business and many others. Therefore, it is necessary for Computer Systems and Information Security department to initiate motivation schemes to appreciate users' contributions to computer security (Herold 2005, p.35). Users tend to behave positively when they know the return of their participation.

"Engagement communicates management's respect for individuals and their ideas."
(Kim & Mauborgne 2003)

In their three principles of *"fair process"*, Kim and Mauborgne (2003) insist on employees' involvement in making decisions that directly affect them. However, this is opposite in security paradigm. Many organisations ignore users when implementing security policies.

3.7.4 Organisational culture

Central to successful of security awareness programme is the understanding of organisational culture (Chia, Maynard & Ruighaver 2002; Desman 2002; Herold 2005). According to Herold (2005, pp.35-36) many employees fail to comply with security policies because of their task deadlines and/or obeying their managers who tell them to ignore security measures for the purpose of completing a specific task. Following the former reason, management should understand that security comes with baggage and hence they should loosen their controls. The need for periodic updating anti-virus, performing patching and carefully analysing the legitimate of emails and websites all these add responsibilities to employees.

Additionally, and which is more obviously, organisation's support is fundamental factor to all above parameters (Herold 2005, p.35). Enough funds must be allocated to put them into operation. However, it is different when it comes to the real life. According to the survey conducted by D'Arcy and Hovac (2007), security awareness programmes had the lowest score. This suggests that although organisations invest resources in developing security policies, they don't devote extensive resources toward educating users on the importance of compliance (D'Arcy & Hovav, 2007). Management, they see employees' education on security issues as a waste of money. They do not see a tangible benefit out of educating their employees on security issues.

3.8 Conclusion

This chapter aimed at investigating users' involvement in security awareness and the effectiveness of current security awareness programmes in educating users. In the second section, the definition of security awareness and the relationship between security awareness, training and education was discussed where it was pointed out that security awareness is a central to the successfulness of computer security and organisation's prosperity as well. The framework on how to build security awareness programme was described in section three where understanding of organisational culture has been identified as the key to successful building security awareness programme.

In section four, the discussion of current security awareness approaches was presented. Among these approaches are the integration of security awareness materials in employment agreements, face-to-face, games and tools, and web-based. In this discussion users' involvement has been identified as very poor as a result many approaches turn to be rigid focusing only with a subset of users and narrow computer security threats. The discussion of computer security in developing and developed countries was conducted in section five where it has been discovered that most of developed countries are far behind in computer security.

In this chapter, poor security awareness material preparations and deliverance, and ignorance in organisational culture and security culture has been identified as the key factors for the failure of current security awareness programmes. It has been discovered that many organisations buy on shelf security awareness materials without performing need assessment. Moreover, the gap between security personnel and users has also been identified as the driving force for failure of inconsideration of these factors. Therefore, to resolve this, the next chapter provides the discussion of KMS with emphasise on investigating key processes of knowledge management and appropriate features of KMS that will be useful in improving security awareness.

4 KNOWLEDGE MANAGEMENT SYSTEMS

4.1 Introduction

Long before the birth of Knowledge Management, information was the most valuable asset for the success of an organisation. Organisations were striving for efficient and effective use of their information to gain competitive advantage. This was the era of Management Information Systems (MIS). The central processing of information and real time decisions were pertinent attributes of MIS. In contrast, things turned *head-tail* when the concept of knowledge management emerged. The shift for competitive advantage was toward *how's* rather than *what's*. Organisations started to realise the benefit of intangible assets *"Knowledge"* over tangible assets *"information"*.

This was the transition period. Organisations were struggling to shift from *production-based* to *knowledge-based* economy (Kim & Mauborgne 2003). Knowledge economy is a type of economy where employees' ideas and innovations are the catalysts for organisational competitive gain. In this era, employees' *knowledge* became the most valuable asset. Much was invested to attract employees to offer what they have, and encourage the coordination among themselves. Organisations started to look again at their business; barriers between departments begun to be removed, new roles were established, organisations' rules and procedures were distorted or even new ones were created, and new learning culture was introduced. However, to embrace all these new type of support from technology and in particular computing was required.

This is when the other side of the coin appeared. The need for collaboration facilities, wider range of accessibility and ability to store and maintain unstructured information became the crucial attributes for new computer systems. This was the start of the era of Knowledge Management Systems (KMS). KMS have become renowned for their contributions in assisting employees to improve organisation's performance so as competitive advantages. Implementation of K'Netix in big organisation like Buckman Laboratory is the implication of the benefits of KMS (Rumizen 1998; Bernard 2006). On the other hand, computer security has been recognised into ensuring the privacy of organisational knowledge (Randeree 2006). Therefore, since KMS have proven to be

successful in organisations' performance and computer security has been recognised in ensuring organisational knowledge, then why not channel these two paradigms into improving computer security awareness as well?

This chapter will investigate features of KMS and prerequisites for their implementations in the context of computer security. To accomplish this, an extensive literature will be covered to analyse Knowledge Management and its processes, difficulties among these processes, available solutions to these problems and the role technology plays. This chapter will conclude by highlighting useful features of KMS in improving security awareness and its prerequisite for implementing it.

4.2 Knowledge Management

There is no doubt about the successfulness of KMS in improving organisational performance. The antecedent behind this is the growing nature of technology (Marwick 2001). The growing pool of Web 2.0 applications such as Wiki and Blogs introduces more functionality that facilitates knowledge sharing in an enterprise wide. O'Leary (2008) has discussed a lot about how Wiki can be a useful tool in facilitating knowledge sharing within organisations. The existence of *ICN ShareNet*, a global intranet of Siemens and *Connect tool* of BP are such examples of KMS that facilitates collaborative events (Andriessen & Huis in 't Veld 2001).

However, before the implementation of any KMS it is important to clearly understand the key concepts of knowledge management, the activities of knowledge management and how KMS facilitates these activities. Understanding Knowledge Management processes, organisational cultural barrier, and organisational learning environment are fundamentals for a successful implementation of KMS. Furthermore a KMS is to work well within an organisational culture and support organisational learning, then understanding the organisation is crucial.

Fundamental to KMS implementation is the understanding of Knowledge Management processes (KM processes). KM processes explains pertinent procedures to be followed to capture and make an effective use of employees' knowledge. However, rushing into discussing Knowledge Management processes without a proper understanding of its

ingredients might lead to divergence of the concept. Therefore, this section will begin by explaining what is meant by knowledge and Knowledge Management and finalise with the core KM processes.

There is no single definition of *knowledge*. Depending on organisation's perspectives, knowledge can be defined in different ways (Fairchild 2002). There are those who associate *knowledge* and *information*, and those who deny. Stenmark (2002) argues that *knowledge* cannot be separated from its *knower* and *"what can be articulated and made tangible outside the human mind is merely information"*. On the other hand, Marwick (2001) describes knowledge as experience and understanding of employees in the form of information artefacts, such as documents and reports. However, whichever the case knowledge is not information (Lang 2001). Information is all about facts while knowledge is the combination of experience, heuristics, and owner's beliefs (Nonaka 1994). However, the differences between knowledge and information are beyond the scope of this section, much has been discussed by McDermott (1999) on their differences. Therefore, whatever the organisations' perspectives about knowledge are, what is fundamental for KMS' implementation is whether knowledge can be transferred from its owners into a computer system in a useful form.

Knowledge can be categorised in two forms: tacit and explicit. What has long been built in human brain through experience or learning is categorised as tacit knowledge (Marwick 2001). This type of knowledge is highly unstructured and difficulty to maintain. On the other hand, the tacit knowledge that has been codified or extracted from human brain is what considered as explicit knowledge (Marwick 2001). This type of knowledge is highly simplified and easy to be maintained. All these forms of knowledge are essential when it comes to organisation's performance. Further distinctions between tacit and explicit knowledge can be obtained from Table 3.

Tacit Knowledge (Subjective)	Explicit Knowledge (Objective)
Knowledge of experience (body)	Knowledge of rationality (mind)
Information	Knowledge
Simultaneous knowledge (here and how)	Sequential knowledge (there and then)
Analog knowledge (practice)	Digital knowledge (theory)

Table 3: Types of Knowledge
(Adapted from (Nonaka & Takeuchi 1995, p.61))

As organisations started to realise the contribution of knowledge in performance increase and competitive advantage gain, knowledge management became an organisational issue (Folkens & Spiliopoulou 2004). The focus was to collect, integrate and reuse what an employee knows to bring about innovation and performance increases in an organisation (Kim & Mauborgne 2003). Moreover, due to competitive nature of the market, organisations need to be safe with their intellectual property *"knowledge"*. Therefore, by capturing what is in employees' head, organisations are positioning themselves in a safe side.

However, as with the difficulties in defining knowledge, Knowledge Management also has different perceptions. There are those who define Knowledge Management in technological, sociological, and organisational perspectives (Tochtermann, Dosinger & Puntschart 2004). Techno-centric focuses on tools and techniques to make Knowledge Management happen while social-centric emphasises on human resources. Moreover, organisational perspective sees knowledge as performance equalizer. However, since computer security focuses on improving performance of an organisation and protecting an organisation from external and internal threats, therefore organisational perspective is most valuable to this dissertation and will be discussed in more detail.

Unfortunately, knowledge is messy (Allee 1997), it is tough to isolate Knowledge Management from Sociological, Psychological and Technology disciplines (Falbo, Arantes & Natali 2004). It is nearly impossible to talk about Knowledge Management without associating it with human elements. Likewise in technology, though

Knowledge Management is about people, but they need technology for effective communications (Rao 2002). Moreover, central to successful Knowledge Management is organisation's support; therefore the organisation places itself at the centre of Knowledge Management (Rao 2002).

4.2.1 Knowledge Management processes

Knowledge exists in many forms and derived from different sources within organisations; human, e-mails, reports and many alike. Moreover, different roles demands different knowledge (Andriessen & Huis in 't Veld 2001). The knowledge required by senior managers is quite different from those required by subordinates. Furthermore, knowledge like any other asset expires (Nonaka 2005, p.188). Therefore, it needs to be updated frequently to reflective the current organisational needs. In the context of security, the knowledge that required by end-users is quite different with those required by top-managers and security personnel as well. All these are issues that need to be addressed in any KMS developed.

Many researchers have described knowledge management with different processes. Benbya and colleagues (2004) describes knowledge management into four processes; knowledge generation, integration, sharing and dissemination. Moreover, Alavi and Leidner (1999) express knowledge management in four phases; creations, capture, integrate and transfer. However, regardless the broadness of the description of knowledge management processes, they all have a common perspectives. Therefore for the purpose of this dissertation, four knowledge management processes will be considered; knowledge *capture*, *organise*, *store* and *share*, see Figure 7.

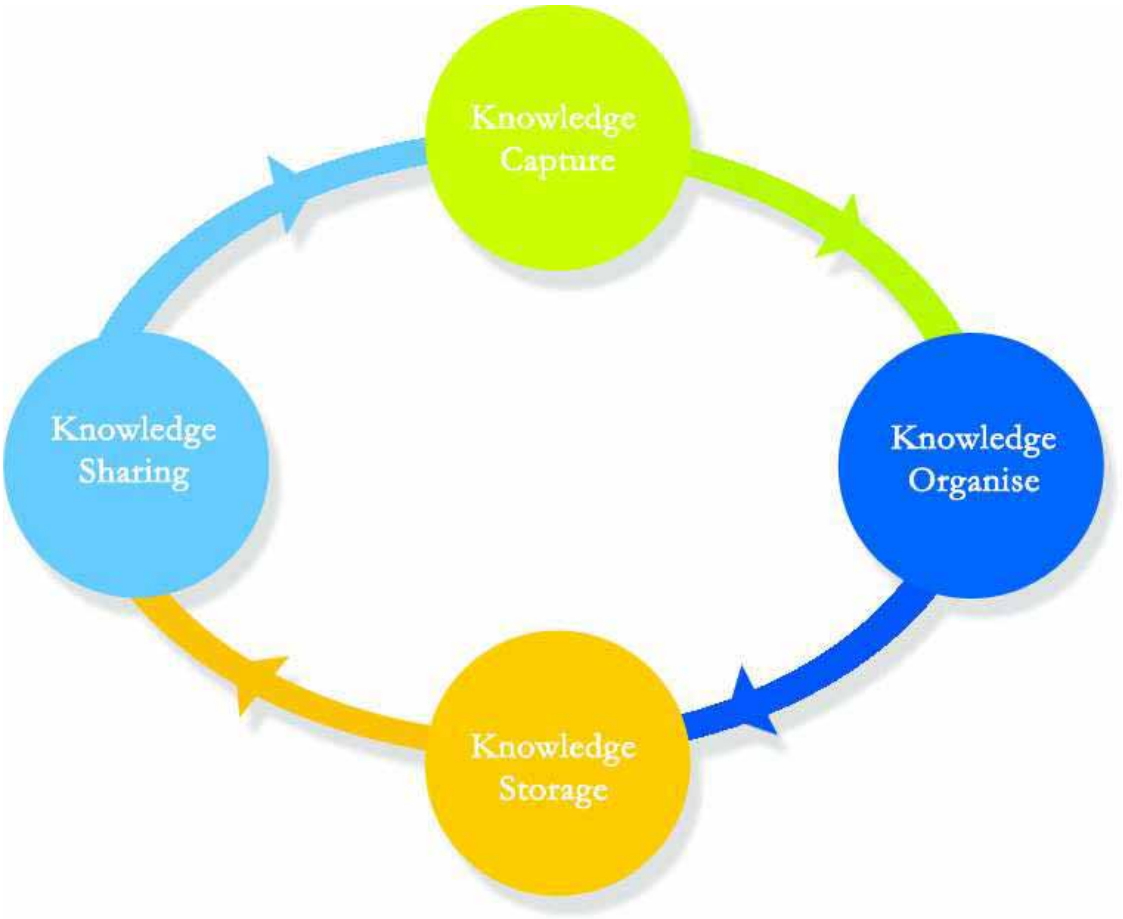

Figure 7: Knowledge Cycle

Knowledge Capture

Word processing has contributed much in knowledge capturing (Marwick 2001). It is through word processing that we are writing and learning in colleges, project teams are exchanging ideas through report and many alike. Knowledge capturing can be defined as the process of articulating tacit knowledge from organisational *knowledge worker* and/or external sources into a more persistent form that can be used in future(Marwick 2001; Nonaka 2005). However, technology is moving fast. Currently there are many automated tools that can capture the *know-how* of knowledge worker for future use. The emergent of voice recognition is a good example of these technologies (Marwick 2001).

However, there are barriers that must be overcome to convince *knowledge worker* to share their knowledge. Knowledge workers tend to be busy, so they do not have

enough time for socialisation or collaborative events. Moreover, the rigid organisational culture that does not entertain social interactions also has impact on knowledge sharing with organisations (Nonaka 2005, p.188). However, all these can be resolved by changing organisational culture by shifting to learning culture, and by introducing incentives to motivating knowledge workers to uncap their knowledge.

Knowledge Organise

As it was mentioned previously, articulated knowledge needs to be stored for future use. However, prior to its storing, it need to be organised so as to facilitate easy retrieve. Rao (2002) emphasises on the quality of knowledge content so as to reduce content search time that can have negative impact on *knowledge seekers*. Moreover, Alavi and Leidner (1999) commented on necessity for knowledge integration and organisation in increasing organisational competitive advantage.

Knowledge Storage

Now that tacit knowledge has already been articulated and content has already organised based on the domain, the next process of knowledge management is to store the content in the format that can be inferred in the future. However, this process resembles much with knowledge capturing. Unlike knowledge capturing, knowledge storing take a steps further into providing security mechanisms in the environment where there are many number of users. Moreover, knowledge storing provides indexing mechanisms that facilitates easy retrieval of knowledge content. On the other hand, knowledge capturing can be a traditional method of capturing tacit knowledge by observation which it is hard for reusing.

Nonaka (2005, p.188) emphasises on context management of the stored knowledge content. In knowledge storing it is not about how huge your knowledge repository is. The crucial bit is the enough availability of knowledge context. This view is inconsistent with Allee's view that the more you pin down knowledge the more it slips (Allee 1997). According to Nonaka (2005, p.188), poor contextual details of knowledge content, it is viewed as being lost. Therefore, this emphasises on the balance between the captured knowledge and the stored knowledge. Knowledge content must not be summarised to the extent to loose its meaning.

Knowledge Sharing

This is the backbone of knowledge creation (Nonaka 1995, p.56). According to Alavi and Leidner (1999), knowledge is useless if it is not shared. The captured, organised and stored knowledge must be accessible to employees at large to stimulate new insights and innovations so as to improve the productivity of the organisation. Knowledge sharing involves trust between employees (Lang 2001; Rao 2002). Again this is an organisational culture problem. As it was explained previously, organisations should encourage knowledge workers by introducing recognition award and loosening it cultural norms.

Knowledge sharing involves knowledge searching and retrieval. There are two mostly deployed model for knowledge retrieval; *push* and *pull* (Alavi & Leidner 1999; Nonaka 2005). The pull model is a traditional model that involves search for and retrieve of knowledge based on specific content keywords, while in push model *knowledge seeker* is being notified on the posts of new knowledge content. For instance, in Wiki based collaborative KMS, when a new member adds comments or new content, each member is informed about the new *"arrival"*. On the other hand, the former approach members do not receive any notifications about the content.

4.2.2 Knowledge transformation process

Central to the successful of organisation is how people exchange information and communicate with one another in everyday company life (Davenport & Probst 2002, p.111). This information, in terms of knowledge, comes into different forms and members exchange this information in different ways. Employees interact with KMS either as knowledge *provider, seekers* or *intermediaries*. Knowledge between them circulates in different formats. Knowledge seekers retrieve articulated knowledge while *providers* share their tacit knowledge with *intermediaries* ready to be fed in KMS. Therefore, it is crucial to understand how different forms of knowledge can be transformed within an organisation.

.

As mentioned previously, knowledge can broadly take two forms; tacit and explicit. Tacit is what resides inside human brain while with explicit, it is any form of knowledge that has been articulated from human brain (Marwick 2001). Furthering the

notation of tacit-explicit, Nonaka and Takeuchi proposed a knowledge-conversions model called SECI which has four processes, see figure 8 (Nonaka & Takeuchi 1995, pp.56-94). The model elaborates how different forms of knowledge can be captured and created between employees within an organisation (Nonaka & Takeuchi 1995, p.57). Therefore, it is worthwhile to bring its discussion in this section because for a successful building KMS an understanding of how knowledge circulates within the organisation is crucial.

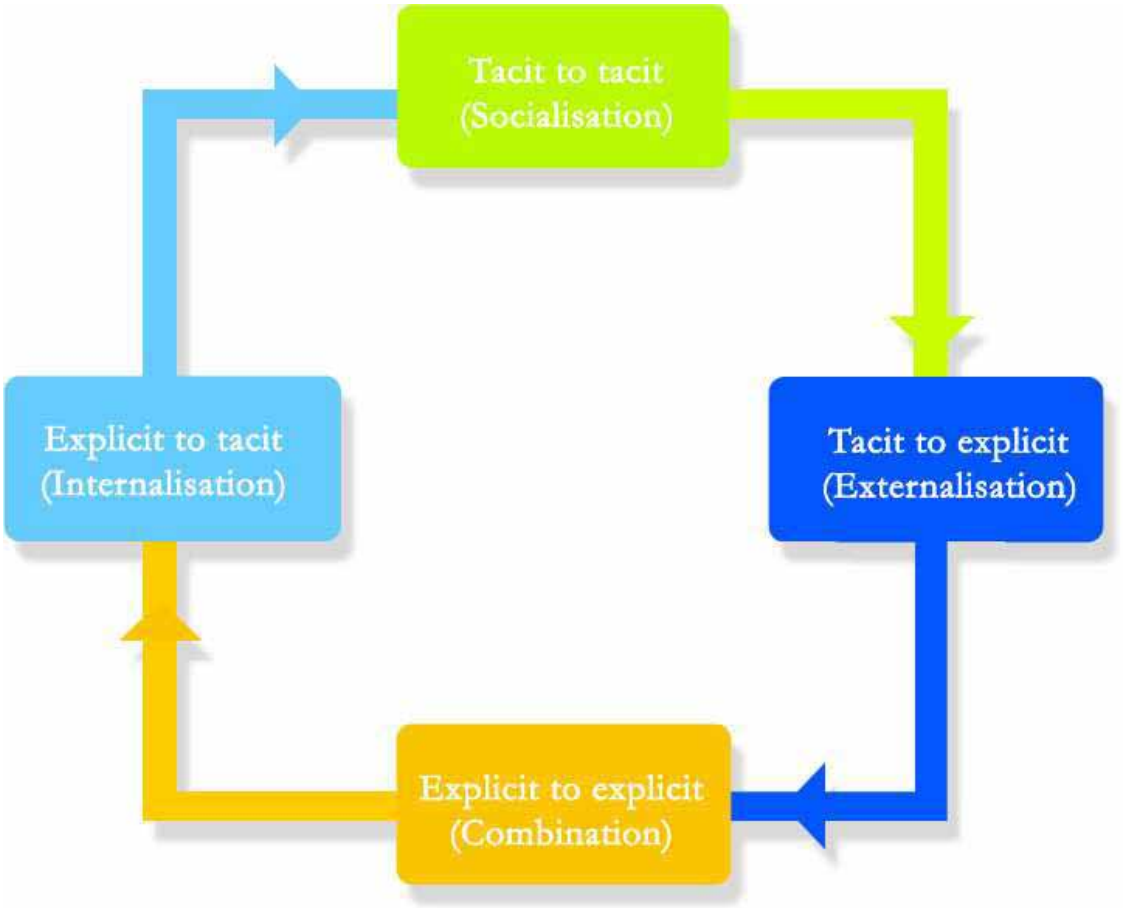

Figure 8: Spiral of knowledge

Socialisation

Nonaka and Takeuchi (1995, p.62) defines socialisation as the process of creating knowledge among employees by sharing their tacit knowledge. They went further and ascertained that in this process knowledge can be shared within employees without using any language. However, their view conflicts with Allees' view (1997) that knowledge travels via language, therefore without language it is impossible for

knowledge sharing. Nonaka and Takeuchi overlooked that evening eyes blinking is also a form of language. Therefore, following this view, it is correct to say that tacit knowledge can also be shared without speaking or writing, but instead through observation and practice (Gronau, Muller & Uslar 2004).

Knowledge is self-organising; it needs clear boundaries for it to succeed (Allee 1997). On the other hand, management *buy-ins* is crucial for establishment of the clear path for knowledge to flow within organisation (Bixler 2002). Therefore, it is necessary for organisation to understand the needs for social activities within organisation. Much can be exchanged during coffee break; employees have a good chance of exchanging what they know during these meetings. Furthermore, this phase can be useful to determine who shares what with whom.

Externalisation

In ex*ternalisation phase* tacit knowledge is converted to explicit knowledge. This is when one tries to express her idea about something by either writing it down in plaintext, drawing sketches, models or metaphors (Gronau, Muller & Uslar 2004). A very common example of this form of knowledge conversion is during seminars or proposal presentations. This is when knowledge can be captured for future use in creating new insights (Nonaka & Takeuchi 1995, p.66).

However, this should go in parallel with the type of audience. Different user category requires different approaches of material deliverance. Therefore, it is necessary to understand the type of audience before planning for material to be delivered. This directly associates with designing of KMS because one needs to understand different mode of material presentation for targeted users.

Combination

Explicit knowledge exists in different forms in an organisation. They might be in email as plaintext, images and/or video (Nonaka & Takeuchi 1995, p.67). In this phase, these different formats of explicit knowledge are reformatted and combined to form more meaningful knowledge. For instance, when systems analysts meet with designing team, they combine their conceptual system models to form a blueprint of the final system.

This phase is essential in security context where different explicit knowledge from different sources will need to be combined to educate users on security threats. These sources might be external security experts, public security websites, anti-virus software vendors and many alike. All these sources have different forms of explicit knowledge. Therefore, this should be taken into account when designing KMS.

Internalisation

This is *explicit-to-tacit* knowledge conversion. What has been articulated and stored in knowledge base need to be accessed and probably create new insights. The tacit knowledge that has been digitised from externalisation and combination phases is accessed by other employees to help them deal with the problem in hand. This is what is termed as *learn-from-past*.

However, this directly associates with the knowledge content. Rao (2002) emphasises on organisational participatory approach in validating knowledge content. It is this content that determines the successful of KMS. Knowledge is made for people therefore it should reflect their needs by having relevant material.

4.3 Organisational learning

In the previous sections, section 4.2.1 and 4.2.2, much has been discussed about *what* it takes for knowledge to be shared and created among employees. However, there is a lot to knowledge sharing and creation. There must be a favourable environment that will enable smooth knowledge sharing. This section focuses on *how* to go about getting employees to participate in making organisation knowledge being utilised to its perfections.

In an organisational context, knowledge is useless without sharing, so as in information security (Alavi & Leidner 1999). Introducing computer security to employees' daily activities is like adding burden to their tasks. Without proper arrangements to prepare them in participating in computer security knowledge sharing, things could fall apart. Therefore, it is mandatory to understanding the ingredients of

organisational learning so as to combat ourselves with the heavy task that we have ahead of us.

4.3.1 What is organisational learning?

Prior to delving into the ingredients of organisational learning, it is crucial to clearly understand what it meant by organisational learning. The term organisational learning and learning organisation are used interchangeably. While learning organisation express the environment where learning activities are undertaken, organisational learning express the actual process of learning (Denton 1999, p.16). Denton (1999, p.17) defines organisational learning as the process of improving actions through which new ideas and innovations are built and shared to create better knowledge and understand. However, the discussion on what constitutes learning organisation and organisational learning is beyond the scope of this section. This section will only concentrates on what constitute on organisational learning.

Nonaka and Takeuchi (1995, p.44) proposed two types of learning activities. They argued that the first learning activities concentrates on creating *know-how* for specific problem domain while the second type of learning involves establishing new beliefs to wipe out the existing ones. However, for the purpose of this dissertation all these types are of importance since employees within an organisation need to be combated with specific knowledge of fighting against computer threats while they also need to pass past their previous beliefs that computer security is not of their concerns. In short, organisation that need to improve its performance it must introduce learning environment that will change its employees from being egocentric to altruistic.

Denton (1999, p.20) proposed six reasons to why an organisation should shift to learning process. These includes shift to production factors, acceptance of knowledge asset, volatility nature of business, dissatisfaction among managers and employees, the increase of competitive nature and high customers' bargaining power. All these reasons are applicable to the problem domain of this dissertation. However, the volatility nature of business fits more with computer security domain. Computer threats are evolving in unimaginably speed.

4.3.2 Senge's organisational learning process

Understanding what it meant by organisational learning, and its difference from learning organisation is not enough to introduce learning process within an organisation. Having spotted this illness, Senge (1990) proposed a practical approach of organisational learning model. According to Senge, for an organisation to shift to learning environment it needs to undergo five steps. Therefore, the whole of this section will concentrate on exploring what constitutes in each step. However, it should also be noted that the order in which these steps are does not matter.

- ***Personal mastery***

Lang (2001) argues that *"It is knowledge that holds a firm together"* and organisations learn from employees' participation in communities that have philosophy, practice and formal means of communication. It is therefore prudent for organisation to understand employees' contributions in organisational competitive gain, and support these communities. However, employees also must play their role in participating in their growth and development plans (Senge & Audio 1990).

Dervitsiotis (1998) defines personal mystery as a *continually* discipline of sharpening our knowledge. It is clear from the definition that emphasis is on *ever-ending* process of learning. However, as previously pointed out, organisation's management must appreciate employees' contribution by facilitating learning activities, while on the other hand employees are responsible for participating in learning process. Therefore, the process of knowledge creation relies on employees with little input from management.

- ***Shared vision***

"...share knowledge involves uncapping our thinking processes for others in the present moment" (Lang 2001). This statement emphasises on community consciousness. If employees open to others what they think it is valuable for organisation, they can share and discuss different views and come up with a community decision *"shared vision"*. In other words, shared vision is a common view for community members.

Senge (1990) argues if there is shared view, employees feel the sense of ownership and thus lead to unlocking of their ideas and open the gateway for innovations. This discipline has some affinity with three principle of fair process (Kim & Mauborgne 2003). The principle emphasises on employees' engagement, explanation and expectations clarity. Engagement emphasises on employees participations, while explanation emphasises on awareness and expectations clarity emphasises on management decision stability.

- ***Mental models***

According to Senge (1990, p.235) mental models are the image, assumptions and stories which we carry in our mind. It is this models that make people judge things differently. Mental models associates with human belief and it is this belief that change the attitude of someone. Mental models are also generative (Senge 1990, p.242). However, mental model are difficult to exercise, it need a plenty of time to create and master similar views in a team.

- ***Systems thinking***

"...find a solution, not culprit" (Senge & Audio 1990). Do not delve to wash oil drop from a car without knowing the hole and root cause of it. This discipline emphasises on finding the solution to a problem and not solves the problem at first glance. This discipline is similar to *Root Cause Analysis*, a problem solving technique that emphasises on determining the original cause prior to solving the problem. .

This is the core of organisational learning. All disciplines we have so far explained are not enough without system thinking. As emphasised by Senge (1990), system thinking discipline is a fusion point of other remaining disciplines.

- ***Team learning***

According to Senge and Audio (1990) team learning is the process of aligning and developing the capacity of a team to create the results its members truly desire. Senge (1990), argues that team learning has three critical dimensions in organisation; the need to brainstorm about complex problem, creating innovations and as the member of other learning teams. However, there is no such morale within organisations. Team learning fits in sports like teams.

Contrary, Senge (1990) argues that with this nature of business, team learning is badly needed within organisations. He emphasises that the successful of an organisation is dependent to the successfulness of such teams within the organisation.

Now we know what knowledge management, with its processes, is capable of. We know many, if not all, barriers that can hinder us from utilising the fruits of knowledge management. Fortunately, Senge has provided us with the way to overcome these barriers. However, the problem still persists; how can we apply Senge's discipline to overcome these barriers? Nonaka (1994, p.188), proposed the introduction of community of practice as a solution. Therefore the next section will discuss how community of practice can resolve these barriers.

4.3.3 Communities of Practice

For an organisation to be successful knowledge must be shared within its members, knowledge that is not shared is useless (Alavi & Leidner 1999). But the problem is, how can an organisation make its employee share what they have? Through motivating them with rewards, or impressing them with sophisticated technologies? Though all these approaches have credibility, employees tend to learn more through participation in small groups of people who interact regularly (Davenport & Probst 2002, p.108). Therefore, it is necessary for organisation to understand and support human relationships within their organisations.

The phenomenon of Communities of Practice (CoP) emerged in 1990's when a study to investigate group of Xerox technicians proved that employees tend to behave differently when they work into groups (Davenport & Probst 2002, p.117). The study showed that there are differences between work procedures and the actual working procedures. The study explained Xerox's technicians when faced with technical problems. Technicians tend to ignore technical manuals and instead seek for help from their colleagues (Davenport & Probst 2002, p.117).

Knowledge is about people, if well managed then they will be able to share what they have and adopt that trend. Allee (1997) argues that *knowledge seeks community*.

Moreover, Lave and Wegner (1991) defines community of practices as collaborative, interactive networks of individuals who have the same mission of learning about a problem domain of a specified scope. All these emphasise on the fact human relationships within organisations is a crucial attitude to practice. To emphasise on this, Lang (2001) argues that in order for organisation to succeed, Knowledge Management should exhale its boundaries and establish human relationship.

Lave and Wenger (1991) argues that CoP can be differentiated from ordinary communities like groups or teams by three unique characteristics; domain, community, and practice. *Domain* explains the scope of the community whereas *Community* explains the way member of the community gather to discuss their matters. Moreover, *Practice* explains specialisation of the community. These characteristics differentiate CoP from other communities because in groups like team-fans they do not have common practices.

For instance, the CoP formulated by Knowledge Mapping and Structuring Unit at Unilever originated from *food production* company with the aim of enhancing efficiency in production and improve innovative processes. The CoP was organised due to the need of new *production*. After member being assigned, they were brought in a one week *workshop* to discuss different strategies in solving the problem at hand (Andriessen & Huis in 't Veld 2001). The *italicised* words explain the domain, practice and community of the CoP as proposed by Lave and Wenger (1991).

CoP can be formulated using two approaches; bottom-up and top-down approaches. Davenport and Probst (2002, p.109) explains bottom-up approach as a CoP initiative that lead to the establishment of a formal CoP within an organisation. This explanation can be associated with the establishment of central office for the interlinking of knowledge management activities at Siemens. At Siemens, this approach was initiated by informal committed members of Knowledge Management staff. This approach normally has positive feedback because they are initiated by the doers.

On the other hand, top-down approach is the CoP initiative from top managers to subordinates. This explanation can be associated with Unilever CoP (Andriessen & Huis in 't Veld 2001). At Unilever, management prepared a team by selecting on expert

who is committed and ten to twenty other members to join the CoP. However, this approach mostly fails because employees feel to be dragged, unless the management is smart enough to know when and how to formulate the CoP.

Since CoP comprises of members with specific objectives, therefore to establish CoP there must be some processes to be followed. Whatever the approach, bottom-up or top-down, there are must be an initiator of the community who needs to *sale* his idea about what he intends to do and for what purpose. If other employees *buy* the idea, then follows the actual execution of the community. However, the execution of the community need to be evaluated, if it meets the CoP's objectives and fulfils members' desires then the community continues to operate, and if not then it has to end.

These processes are what Davenport and Probst (2002, p.109) referred to as CoP lifecycle. In their explanation, they suggested that a CoP falls into three phases for their operations. As it can be seen on figure 9, CoP comprises of three phases; start-up, run and improve, and wind-down phase, each with different operations. The explanation of each phase will be provided below.

Figure 9: CoP Lifecycle
(Adapted from (Davenport & Probst 2002, p.149))

- ***Start-up***

This is the awareness phase where members of the community are being told the purpose of the CoP and its scope. This normally is being done by base members of the community. The community leaders are being selected and members establish their mode of conducting their meetings. Though, if the community is virtually, instead members will define the technology to assist their meetings.

- ***Run and improve***

This is the operational phase. This is when the community come into actual execution of the community. This is the actual knowledge sharing and creation phase where members meet for solving the problem in hand. However, constant monitoring of the community will be performed in this phase to make sure it operates with its objectives.

- ***Wind-down***

Community should exist as long as it serves its purposes. Based on the evaluation, the community may be closed down and the knowledge created in the knowledge base copied and transferred into another CoP or being stored for future use. Meanwhile, if the community happen to fulfil and excel its objectives then it will continue to exist.

4.4 Computing for Knowledge Management

Knowledge is power and by sharing we add more into it. Consider a very simple scenario where employee 'A' happens to have a problem in login into her account and after consulting employee 'B', he discovered that the problem was a buffer overflow. After a simple demonstration from employee 'B', she managed to fix the problem. From this scenario, two components of Knowledge Management are regarded to be essential for performance improvement; *knowledge sharing* and *creation*. Employee 'B' agreed to share his knowledge about how to clear buffer overflow while employee 'A' learned how to fix the problem so it would not bother her if it happens again.

However, two essential questions arise from this scenario. The first question is how do employees communicate their problems with their colleagues, and second, if they manage to communicate, in whichever way, how is the shared knowledge going to be captured for reuse? This adds a third component for improving organisational performance; *knowledge reuse*. Knowledge is a valuable asset that needs to be managed like, or even more than, any other assets. Today employee 'B' is there to answer the queries, but what about tomorrow? Would he be there when he is needed?

"Prevention is better than cure"; it is a common axiom that we have been gossiping in our life, but yet we fail to practice its context when it is required to. Tomorrow is beyond our scope; anything can happen. Employee 'B' might quit the job, or even be

in a short holiday where he can not be reached. Whichever the reasons, proactive measures must be taken by making *"back ups"* of whatever has contributed to the improvement of organisational performance. However, this does not only put the organisation in a safe side, but also quantifies organisation's capabilities. From the *"backups"*, new strategies can be initiated.

Although knowledge *sharing*, *creation* and *reuse* have been identified as fundamental components for performance improvement, still there are a lot that need to be done to *make them alive*. Organisational cultural change is of the most common prerequisite for their effective execution. The barriers between employees must be resolved; they should be opened and understand the benefits of sharing. However, the organisational cultural change is beyond the scope of this section, only *enablers* of the identified components will be discussed in this section.

Unfortunately, you can not make somebody to create new *knowledge*. The process of *knowledge creation* is the association of learning process and the learner. Therefore, the process of *knowledge creation* is ignored in this section. In other words, there are no technological enablers for making someone instil new knowledge. This section will conclude by identifying the roles technology plays in enabling the execution of these components as recognised in literature.

4.4.1 Computing overview

Prior to answering the questions arouse in the previous scenario, it is worthwhile to investigate what it meant by computing and identify generic roles of computing in Knowledge Management. Fairchild (2002) defines Knowledge Management *enablers* as structures and attributes that must be in place for a successful knowledge management program. Although KPMG (2000) and Rao (2002) proposed eight enablers of knowledge management, this section will only concentrate with technological enabler.

Building on Oxford's definition, computing is the action or practice of using computers. Computer provides massive storage of data and high processing speed. Incorporated with its applications, intranet, internet and other web applications,

computers reduces the gap of space and hence makes communication easier. In summary, computers can provide massive storage of information, high information manipulation speed, and global communication and also provides with searching capabilities which can be useful if applied to Knowledge Management processes.

It is true that knowledge sharing can stand on its own without the help of technology. However, to be effectively technology must be there to support its capture and organisational wide accessibility (Rao 2002; Alavi & Leidner 1999). Stenmark (2002) argues, *"...for KMS to be successful they must include users and provide mechanisms for these users to locate and interact with each other"*. The issue of technology resonates most in an enterprise environments where knowledge need to be centrally stored and its accessibility need to be enhanced to reach employees at large.

The concept of computing for Knowledge Management can be explained using C3S model as proposed by the author (2008). In his work, the author described four roles computing plays in Knowledge Management; capture, store, search and share, as shown in figure 10. This view is in the same line with that of Alavi and Leidner (1999) that Knowledge Management requires database and database management, communication and messaging, and browsing and retrieval technologies. However, they ignored the technology for knowledge capturing.

The first component of the C3S model is *Capture* which reflects the category of technologies that are useful in knowledge acquisition process, these includes video and audio capturing devices. The second component is *Store* which presents all technologies that are useful in knowledge storing, these includes knowledge base, data management systems. The third category, which includes expert locators and yellow pages, are represented by *Search* component of the model. The final component, *Share*, reflects all collaborative technologies that assist in knowledge sharing, these includes Web 2.0 applications and intranet.

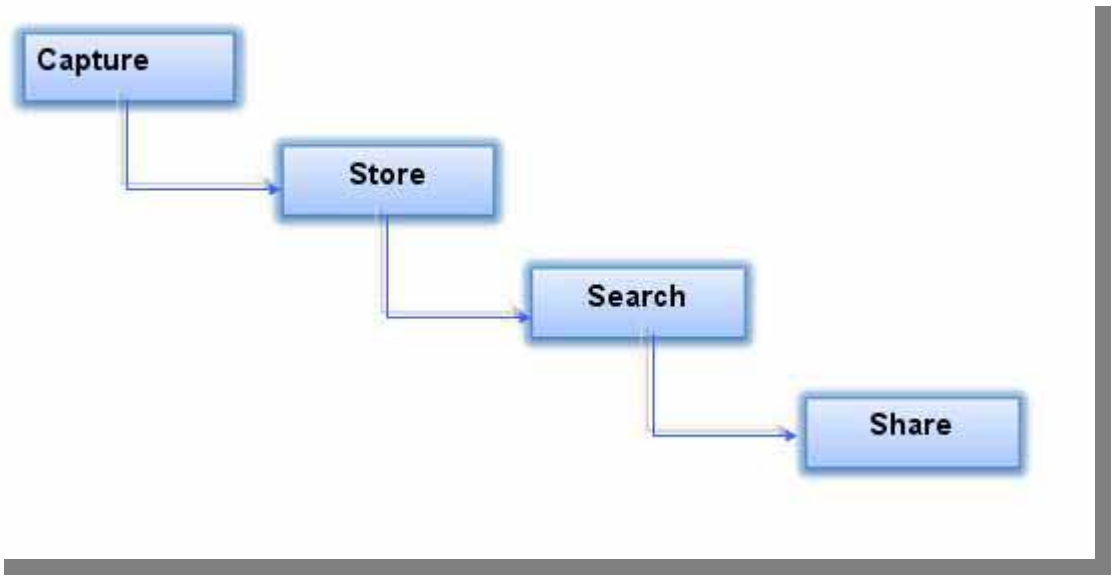

Figure 10: C3S Model

However, both these technologies can be combined into two categories. Hansen and colleagues (2005) argues technology can support Knowledge Management in two basic approaches; codification and personalisation. In codification, unstructured knowledge is transformed and stored into common format for future use. It combines all technologies that fall under Capture and Store components of C3S model. This approach proves to be more useful because it build a gap between capture and store; once knowledge has been captured it has been stored already. However, it is also should be noted that knowledge capturing does not always implies that knowledge is being stored.

Moreover, personalisation approach focuses on enabling two parties to communicate by both providing means of searching for experts and direct communicating with them. Again this approach proves to be useful because it plays twofold roles. Firstly it allows for expert searching and secondly it enables two parties to directly communicate. The C3S model considers search and share as two separate entities, but logically we search for expert because we want to communicate with them. Therefore, these two components must go hand to hand.

However, the codification approach is dependent to personalisation approach. If for instance Web 2.0 is applied as the means of establishing communication between two

ends, therefore the knowledge will be stored in the form of plaintext, video and audio but it differs when the technology changes. If the technology applied change to, for instance video and audio capturing systems, then text format would not be applicable. Therefore, based on the above exploration, the approach proposed by Hansen and colleagues (2005) will be applied as a guideline for answering the questions below as aroused from the scenario of section 4.4.

4.4.2 How do employees communicate their problems?

This question can be answered by the personalisation approach. As previously explained technological enabler in this question serves dual roles. Firstly, by providing employee "A" with search capabilities to search for the right person to consult, and then it enables the communication of the two ends; employee "A" and "B". Mosaic of technological enablers can be applied in this question, these includes expert locator, yellow pages, direct phone line, email and collaboration tools like Web 2.0 and intranet.

Thanks to the advancement of technology. Technology have made the world as a single village, therefore technology removes the gap of space that otherwise would limit knowledge sharing (Marwick 2001). However, mush should be considered for the case of material accessibility and not direct communication with the expert. In enterprise environment where there are many roles and knowledge accessibility is sensitive, there should be a mechanisms to prevent unauthorised access. With User Profiling capability of technology, each user can be assigned limited privileges to access the contents based on their roles.

4.4.3 How is the shared knowledge going to be captured for reuse?

This can be answered with the first approach, codification approach. Recap, in codification, unstructured knowledge is transformed and stored into common format for future use. As previously explained this approach is dependant to personalisation approach. Whichever the technology applied in personalisation approach, the most common technologies are database and database management, knowledge base, knowledge repository, content and data management and many alike.

In an enterprise environment where knowledge comes from different domains, organising of this knowledge is of essential so as to facilitate its fast retrieval (Rao 2002). In associate with this approach, other categories of technologies are being applied. These technologies include taxonomy, thesaurus and metadata. Their main task is content organisation based on domain, practice and owner of that document.

Moreover, knowledge tends to vary with time. What was useful today, tomorrow it might be obsolete. Therefore, codification technologies must be capable to allow these changes. The underlying technology must be able to allow periodic amendments of the content in totality or portion of it. It should also keep track of who, when and where the modifications occurred.

4.5 Knowledge management systems

The economy has changed from product-based to knowledge-based. In knowledge-based economy, knowledge has been identified as a valuable asset to improve organisation's performance and competitive gain as well. However, the challenge arouse on how to convince *knowledge workers* to uncap what they have and share with others in an organisation. In an organisational context, knowledge is limited if it is not shared within employees. Many researchers proposed the need of learning activities to facilitate knowledge sharing. In 1990 Senge proposed a model for assisting organisation to shift into learning organisation.

Many researchers suggest the use of technology to assist in learning environment (Bixler 2002; Rao 2002; Malhotra 2005). Pondering on the matter, author (2008), and Hansen and colleagues (2005) proposed models that can be used to categorise technologies that required for facilitating knowledge sharing within an organisational context. Author (2008) proposed C3S model that focus on categorising technologies for knowledge capturing, storing, searching and sharing. Moreover, Hansen and colleagues (2005) categorised technologies for knowledge codification and personalisation. However none of these models established the connection between technology and KMS as Knowledge Management initiatives. Therefore, this section will focus on exploring what constitute to KMS and its applicable features into assisting knowledge sharing.

4.5.1 Types of Knowledge Management Systems

In an organisational context, KMS are perceived as a central knowledge bank that keeps records of all past successful examples in solving a specific problem (Bernard 2006). Alavi and Leidner (1999) define KMS as a new breed of computer applications that focus on creating, gathering, organising, and disseminating organisational knowledge.

KMS differ from ordinary transactional systems like MIS in a number of ways. Information, which is in term of knowledge, is stored in an unstructured way in KMS (Bernard 2006). Moreover, unlike MIS, there exists only three categories of roles that interacts with KMS; knowledge *seekers*, *providers* and *intermediaries* (Markus 2001). *Knowledge seekers* are those who refer to the already existing knowledge, while *knowledge providers* are domain experts "knowledge workers". On the other hand, *knowledge intermediaries* are those who are responsible for maintaining knowledge content (Markus 2001).

As it was mentioned previously technology plays two essential roles in knowledge creation process. It enables knowledge providers to directly share their "*know-how's*" with knowledge seekers. Moreover, it also enables knowledge intermediary to structure knowledge providers' "*know-how's*" into useful format that can be easily retrieved in future by themselves, knowledge seekers or knowledge intermediary as well.

However, each of the scenarios explained in the previous paragraph depends on a specific or combination of technologies. For instance, technology that can be used for personalisation can never replace the technology for codification, but still they can be combined to operate in ad hoc environment. Therefore it is plausible to understand different categories of Knowledge Management "generators".

Although there are many types of KMS, Bernard (2006) proposed three categories of KMS generators which can effectively be used to categorise KMS. In his article, Bernard explains that generators are the go-by of applications, and are these applications which we are interested with. Therefore, this section the generators

explained by Bernard are going to be used as the framework to describe different types of KMS.

- ***Knowledge repositories***

King and colleagues (2002) defines knowledge repositories as databases that allow the storage and retrieval of knowledge content. These include data warehousing, document repositories, document management system (Hahn & Subramani 2000; Marwick 2001). Davenport, De Long & Beers (1998) went further to categorise knowledge repositories into three categories; external, structural internal and informal internal. External knowledge repositories for the storage of intellectual intelligence while structural internal repository such as research reports, marketing material and techniques and methods. Moreover, informal internal repositories are for storage and retrieval of business best practices (King, Marks Jr & McCoy 2002).

- ***Expert directories***

These are tools that are specifically for finding knowledge workers. These include expert networks, yellow pages, expert database and many alike. Unlike knowledge repositories, expert directory only stores information about the expert (Hahn & Subramani 2000). However, other expert directories both find people with knowledge that one requires and enable it to be transferred to the knowledge seekers. These tools that locate the destination of experts are referred to yellow pages.

- ***Collaborative tools***

These are tools that assist access between users (Hahn & Subramani 2000). These types of tools include discussion forums, Wiki, Portals, video conferencing and many alike. The unique feature that distinguishes this category with the previous is the ability to facilitate collaboration events.

4.5.2 Selecting appropriate tools KMS

Having a tool without knowing where to apply it, it is like the tool does not exist at all. One should understand where it should be applied so as to make it effective. Due to successful of KMS into improving organisation performance, many KM "*applications*" have emerged. However, the burden to select between these tools is left to Knowledge Managers (Hahn & Subramani 2000). Hahn and Subramani argue that

managers need to be directed to what scenario does specific category of KMS is suitable.

Tackling this problem, Kankanhalli and colleagues (2003) proposed product-service approach to assist executives in choosing the right KMS to deploy in their management initiatives. In this approach they associate KMS with the type of the organisation. They classified organisation in two classes; product-based and service-based. They went further and split the organisation in two subclasses; high-volatile and low-volatile. The first category differentiates the organisations based on their nature while the latter classification explains how un/stable organisation is with its nature. Therefore an organisation can be categorised as product-based and high-volatile. This means it is a production organisation that often changes its products.

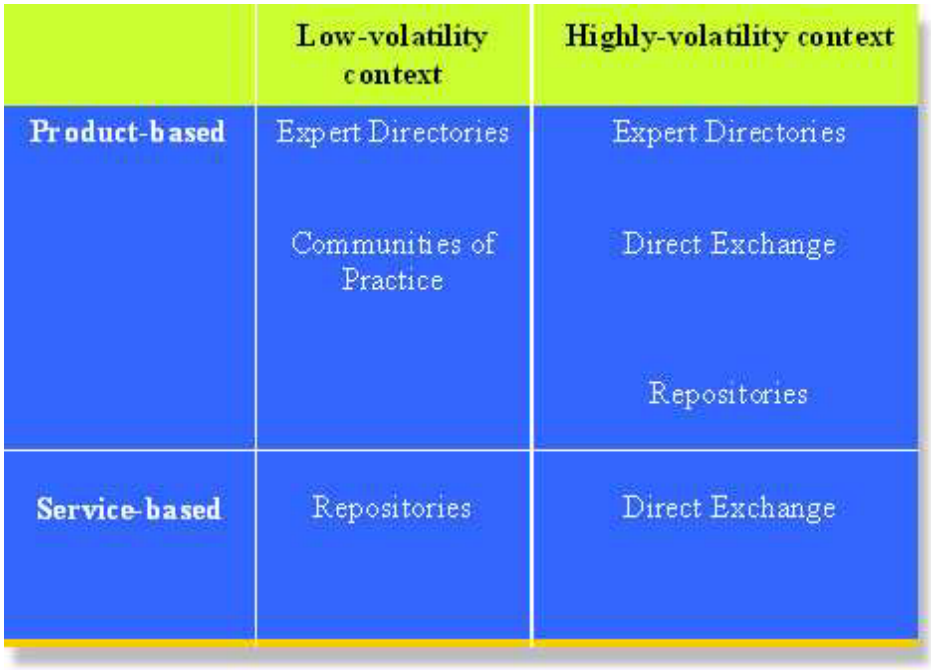

Figure 11: Product-Service KMS Support Model

- ***Product-Based Organisations in Low-Volatility Context***

As shown on Figure 11, this category reflects organisations that their competitive force is based on products. These organisations mainly depend on tacit knowledge and tend to have a lot of informal and formal CoP's. Therefore all organisation that fall in this category, and if they fully depend on tacit knowledge, then personalisation approach is suitable

- ***Product-Based Organisations in High-Volatility Context***

All organisations that operate in an environment where the rate of innovation is high and products are associated with many deadlines, knowledge need to be provided in a real time manner. In this category both types of KMS are suitable to make sure knowledge is available in a required timeframe.

- ***Service-Based Organisations in a Low-Volatility Context***

In this category, the wealth of knowledge accumulated by these organisations and the ability to use this knowledge to serve their clients is a key value proposition. Therefore KMS required in this category is for knowledge content storage.

- ***Service-Based Organisations in a High-Volatility Context***

In this category service is their competitive force and business environment is dynamic. Therefore the time required for knowledge content is crucial. Therefore this approach can adopt personalisation approach like face-to-face communications.

This approach has proved to be useful because prior to selecting for KMS, it considers the nature of the organisation by looking at competitive driving forces. It reflects real operations of the organisations.

4.6 Conclusion

This chapter aimed at investigating key processes of knowledge management and appropriate features of KMS in improving security awareness. The discussion of fundamentals of knowledge management is provided in section two where both knowledge management processes and knowledge transformation process are discussed. In this discussion, organisational culture has been identified as a central to successful of KMS implementation. In section three, the discussion of organisational learning has been conducted where CoPs has been identified as the key solution to overcome organisational cultural barriers in implementing KMS.

The discussion of the usefulness of computing in knowledge management has been conducted in section four where four roles of technology have been identified in relation to knowledge management. These roles include capture, store, search and

share where *capture* describes all technologies that are useful in knowledge capturing, and so forth. The description of KMS and its criterion of selecting what category to be implemented in a specific organisation were provided in section five. In this discussion, three features of KMS has been identified; repository, expert directory and collaborative.

In this chapter, employees' knowledge sharing and the roles KMS plays in facilitating organisational learning have been identified as the driving factors for improving organisation's performance. However, knowledge sharing constitutes many knowledge management processes and different features of KMS apply in different scenarios. Therefore, the next chapter provides the discussion of knowledge management perspectives of security awareness emphasising on how KMS can be useful in improving security awareness.

5 THE KNOWLEDGE MANAGEMENT PERSPECTIVE OF SECURITY AWARENESS

5.1 Introduction

There is no doubt that high security awareness decreases the number of computer break-ins because users starts practicing and applying good security traits (Sharp 2007, p.3). However, there is more into improving users' awareness in security issues than just the dissemination of security policies and expecting users to immediately adopt require practice. From preceding chapters it is evident that many of the issues to be dealt with in security awareness are concerned with the human element and effectively sharing knowledge among the human element and protecting the knowledge of the organisation.

This chapter explores the issues of security awareness and developing security awareness programmes from a knowledge management perspective. The factors which influence security awareness are discussed from knowledge management perspective. Since one of the key areas identified for failure of current security awareness is organisational culture and security culture in particular, this chapter discusses the issues involved and in particular organisational learning in the context of security awareness. The chapter concludes by linking the problems to current security awareness to the appropriate knowledge management issues and activities that can be used to address these.

5.2 Why is Security Awareness a KM Problem?

Shapr (2007, p.3) proposed three factors that must be considered to ensure users are aware with computer threats:

- **Knowledge:** The user knows of the existence of a potential problem with respect to safety or security – for example, she knows that a computer virus may be spread by e-mail;
- **Understanding:** The user understands how to deal with a safety or security problem – for example, she knows that a virus scanner can be used to detect

and remove virus from incoming e-mail, and knows how to install and set up such a scanner;

- **Compliance:** The user acts correctly in order to avoid a safety or security problem – for example, she in fact installs and sets up a virus scanner to detect and remove virus from incoming e-mail.

Senge (1990) emphasises on team learning and shared vision. Team learning emphasises on aligning and developing the capacity of a team to create the desired out, while shared vision emphasise on community view. Therefore, security personnel and users as a team should share their knowledge to create desired output as a team, and they should help each other as a team to build the same view on fighting against computer threats. If they work together as a team, security policies compliance will definitely increase so as computer security.

5.3 Organisational security culture

As it was pointed out in chapter 3, users' are treated as a separate entity when it comes to security. They are not involved when it comes to security decision making. Security awareness materials are prepared without users' input as result security awareness programme(s) turn out to be unsuccessful. On the other hand, researchers emphasises on security and organisational culture consideration when building security awareness programme(s) but things are vice-versa when it comes to actual implementation. Security awareness programme(s) are channelled into communications media that are not convenient for all levels of employees. All these emphasise the gap that exists between security personnel and end-users.

Central to all these is security organisational culture. Organisations need to shift to security learning environment to resolve the gap between end-users and security personnel. The battle between bad guys and good guys is an endless battle. While one side concentrate on providing tight control measures, the other side keeps their eyes wide open to seek for a breakthrough (Robila & Ragucci 2006). Therefore organisations need to build teamwork to harness employees' skills to fighting against this battle (Schlienger & Teufel 2003). If this gap will be resolved then computer

security will be an organisational issue and hence decrease the rate of computer threats and break-ins.

Fortunately, human element is a precious asset in knowledge management. As it was described in chapter 4, central to the success of organisation is employees' knowledge sharing with KMS at the centre of it. Knowledge management emphasises on overcoming negative cultural elements by introducing learning environment, while on the other hand KMS are champions on facilitating learning environment. Therefore, since the solution for failure of security awareness programme(s) is users' involvement in security decision making, and shifting to security learning environment has been proposed to resolve the gap between end-users and security personnel, KMS will then be perfect facilitator for security knowledge capturing, organising, storing and sharing between users and security personnel.

However, it is worthwhile exploring security learning cycles to have a clear picture of what constitutes in it. Therefore, this section discusses Security Learning Continuum as proposed by American's National Institute of Standards and Technology and Security Learning Cycle proposed by Microsoft. NIST's approach is preferred because it is a standard body for American's private and organisational agencies. Therefore it is a good benchmarking. Moreover, Microsoft was included in this section because of the influence it has in computer systems security. The strategies will be assessed and findings will be incorporated into the framework developed as part of this dissertation which will be discussed later.

5.3.1 NIST's Security Learning Continuum

The National Institute of Standards and Technology was originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry's competitiveness; advance science and engineering; and improve public health, safety, and the environment. In 1988, NIST was established by the US congress with the duty to assist, improve, modernise, ensure reliability and facilitate rapid commercialisation of products based on new scientific discoveries (NIST-SP 800 – 16 1998).

The basic function of NIST, of which it is the main concern of this section, is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognised by the Federal Government (NIST-SP 800 – 16 1998).

NIST describes security learning as a continuum. It describes the process of learning starting with security awareness then to security learning and finalises with security education and experience, see figure 12. The model describes the mandatory route to be followed to acquire necessary computer systems' security knowledge. Therefore if someone wishes to change to or being assigned with different role, then he/she must follow the model to acquire necessary knowledge for that specific role.

Since the relationship between security awareness, security training, and education and experience has already been discussed in section 3.2.2, therefore this section only concentrates on their briefly descriptions in the context of this model. However, detailed explanation focuses on the description of the inner-steps between each phase of the model.

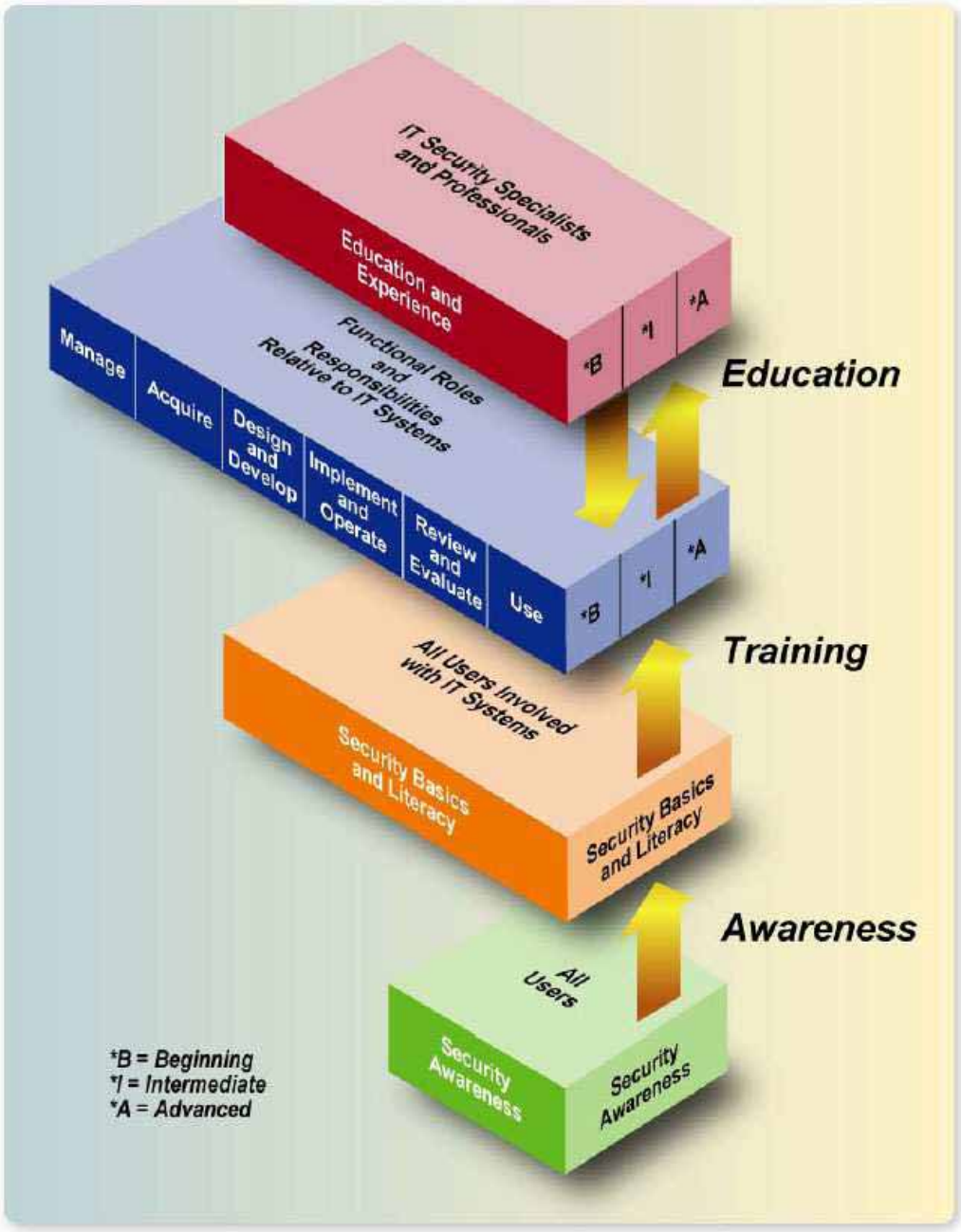

Figure 12: Security Learning Continuum

(Source: (NIST-SP 800 – 50 2003))

As shown on figure 12, security awareness determines execution of the remaining phases of the model. Since the model mirrors necessary steps to be followed to acquire necessary security knowledge, and since it is the first element in the model therefore there is no exception for its attending. Security awareness target all users regardless their roles and expertise. It is this phase where users are being prepared, by changing their behaviours, for the next level of learning continuum.

As it was explained in the previously, security awareness focuses on changing users' behaviour on computer security so as to fulfil defined security requirements. Security training, on the other hand, focuses on imparting users with appropriate knowledge and skills to deal with specific computer systems' problems. Therefore to resolve the knowledge gap, there must be a transitional stage; "Security Basics and Literacy".

Not everybody in the organisation is a computer expert or working with computer systems, unless it is a computer related organisation. In training phase, only computer systems' experts and anybody who interacts with computer systems are targeted. Therefore, "Security Basics and Literacy" focuses in preparing computer systems technical users with basic knowledge and skills that are required to be emphasised in security training. Notice here, the material prepare are also quite different with those used in user awareness phase so as with training material.

After "Security Basics and Literacy," training becomes focused on providing knowledge, skills, and abilities specific to an individual's "Roles and Responsibilities Relative to IT Systems." At this level, training recognises differences between beginning, intermediate, and advanced skill requirements.

The "Education and Experience" level focuses on developing the ability and vision to perform complex multi-disciplinary activities and the skills needed to further the IT security profession and to keep pace with threat and technology changes.

5.3.2 Microsoft Security Learning Cycle

After realising its potentials computer systems security, Microsoft contributed to the body of knowledge by proposing a security learning cycle which intends to assist its customers by providing a security learning framework. This framework can be used by computer systems administrators and security experts as a guideline into building security culture with their organisations. The framework comprises two fundamental components; awareness and training, see figure 13.

The former component focuses on changing user's behaviour (D'Arcy & Hovav 2007; Microsoft 2006) while the latter only focuses on creating new skills (Microsoft 2006).

The first component tells user what and how to meet organisation's security standards and procedures while the second component teaches user with enough skills to deal with specific security problems. As noted by Microsoft, the initial point of the cycle is awareness then followed by training.

Figure 13: Information security learning lifecycle
(Adapted from (Microsoft 2006))

Therefore, based on security learning cycle, knowledge capturing, storing and sharing of KM processes and repository and collaborative nature of KMS has been highlighted as appropriate features for improving security awareness within an organisational context. However, for the purpose of this dissertation, the description of KMS usefulness will focus only on security awareness. *Knowledge capturing* process is useful in articulating security issues from both knowledge seekers and providers while *knowledge storing* is useful for storing security knowledge contents. On the other hand, *knowledge sharing* facilitates searching and retrieving of knowledge content. Moreover, repository nature of KMS facilitates capturing, organising, and storing of knowledge content, while collaborative nature of KMS facilitates the actual knowledge sharing.

From the literature review it was pointed out that user' involvement, poor material preparation and delivery, ignorance of organisational and security culture are among the reasons to why current security awareness programme fail. Therefore, in solving these problems, a KMS framework will be developed to guide the development of KMS in improving security awareness. However, prior to framework development, the results from the survey will also considered on the development of the framework. Thereafter a Wiki-based KMS prototype will be developed to evaluate the contribution of KMS in improving security awareness in an organisational context.

In resolving all these, prior to the implementation of Wiki-based KMS prototype for security awareness, the framework considers computer security perceptions and security culture by including these as factors to determine the level of change management. It is the change management that focus on resolving the gap between executives, security experts and users by educating them the necessity of knowledge sharing and their contribution in corporate security. On the other hand, organisational culture is considered to resolve any conflicts with organisation interests so as to define appropriate type of KMS to facilitate security knowledge sharing between members of all levels.

5.4 Conclusion

This chapter aimed at describing how KMS can be useful in improving security awareness. The second section provided the discussion of why security awareness is being perceived as a knowledge management problem. In this discussion organisational learning as identified in chapter four has been mapped with organisational security culture to allow the applicability of KMS. The discussion of organisational security culture was provided in section three where two security learning cycles were discussed.

In this chapter, knowledge capturing, storing and sharing of knowledge management, and repository and collaborative features of KMS were identified as the key solution to the improvement of security awareness. The next chapter provides the description of security awareness survey emphasising on the roles users play in computer security and the effectiveness of current security awareness programmes in educating users.

6 SECURITY USER AWARENESS SURVEY

6.1 Introduction

Although much has been covered in the previous chapters about the research problem, obtaining industrial views is worthwhile. To achieve this an investigation was undertaken designed with the aim of investigating the roles users play in computer systems security and the effectiveness of current security user awareness programmes into educating users in security relevant issues. To achieve this both questionnaires and structured interviews were conducted and covered both end-users and security experts.

This chapter describes the investigation undertaken, explaining the survey undertaken detailing its structure, respondents and mode of conduct and the results of interviews undertaken. A complete sample of survey will be provided in Appendix A. After data collection, the analysis of the results will be conducted. However, only the analysis of survey questions which have a direct impact on framework development will be conducted. An interview with security expert will be conducted to evaluate the findings obtained from the survey. This chapter concludes by identifying key findings as obtained from the survey.

6.2 Audiences

Since the survey aimed at understanding the roles users play in computer systems security and how different awareness programmes assists in educating users, therefore the targeted respondents included security experts and any computer specialists. However, since a security awareness programme aims at educating all employees in an organisation, end-users also were included. Security experts and computer specialists were preferred because of their broad knowledge while end-users were preferred because they are implicitly integrated in security learning cycle.

Experts were thereafter categorised into two categories, academicians and industrial experts. *Academicians* include university lecturers in Information/Computer systems security modules, and researchers from different computer science research groups

while *industrial experts* include experts and consultants from security and information technology industry. University lecturers in computing department who teach modules other computer systems security were considered to be end-users so as to reduce the biasness of the results. Since the survey was about users' involvement then we need input from them. We need to know their views about their involvement in security.

6.3 Methodology

This survey was done in late June and majority of respondents were academicians with a very small portion of industrial experts. Therefore there were difficulties in physically reaching them since majority of them were out for vacation. This explains to why the questionnaire option was preferred. Although there were interviews over the phone, but these only targeted to a specific small number of security experts.

The survey was based on two questionnaire approaches; offline and online surveying. The first approach was conducted into two phases; the first phase was through physical distribution of questionnaires during the 3rd ICITST seminar which was held on 23rd June 2008 at Dublin Institute of Technology. Moreover, the second phase was based on physical distribution of questionnaires to academicians and experts of different organisations in Tanzania.

The second phase was done when the author was in a short break in Tanzania. Many questionnaires were distributed in different organisations. While in Tanzania, the author was tempted to extend the survey to Kenya and Uganda so as to get the feel of how developing countries perceive the issue of computer systems security. This extension was so potential in this project. The ICITST seminar was one of the potential samples for this survey because it involved experienced researchers and experts in computer science and security from different countries all over the world.

The second approach of the survey was an online survey. This approach was both effective and convenient. It was effective in the sense that it broadens the accessibility of respondents, and convenient because it did not insist on immediate presence of the respondent. Respondent can find and fill in the questionnaire at their time. This

approach had three phases; creating respondents' mailing list, online survey posting and last but not least, survey participation invitation.

In the first phase, two different categories of mailing list were created. The first category was made from academic staff list and second from supporting staff list of institutions and universities of Ireland. After mailing list creation, the survey questions were posted online through an online survey tool, Group Surveys (http://beta.group-surveys.com). This was a very useful tool, it allows respondent to fill in the questionnaire into phases and provides analysis capabilities. Through this tool, a respondent can partially fill in the questionnaire and proceed with it later.

After posting the questions online, the last phase was invitation. The approach was to send email to the mailing list created during phase one of this approach by introducing the host of the survey, explaining its aim and purpose thereafter requesting the respondent's participation in the completion of the survey. The link to the survey was included in the invitation e-mail allow the invitee to access the survey. However, to expand the number of respondents, mailing list from computer security relevant research groups were included. These included *IS World* and *Security Focus* discussion forums.

6.4 Questionnaire Design

Imagine you are given a coffee machine without a user manual and/or being told its purpose. Will it be useful to you? The answer to this question is so obvious, it would not be of useful because you do not know what is it for and how to operate it. Likewise with surveys; without explaining its structure, it might lead to misjudgement of survey results. This section aims at explaining the structure of the survey by going into details of each question explaining why it was preferred and its contribution on the research problem.

Although there were two versions of questionnaires for this survey, only the final structure will be explained since the only difference is the addition of questions. The analysis of the initial offline survey provided some interesting results which prompted the inclusion of additional questions in the second version to further the investigation

and strengthen the results. This section will not only introduce the reader with the structural understanding of the survey, but also acts as a guideline on how to effectively design and construct surveys.

The first section of the survey aimed at understanding the respondents and the nature of their organisation. Different organisations have different needs of security measures. The need of security measures in agricultural and financial organisations is completely different. Moreover, the size of the organisation is also an essential parameter. The larger the size, the higher the accessibility of awareness programmes is required. The first two questions of this section were essential in determining the level of security measures and awareness programmes each organisation requires.

The world is made up of different cultures. The level at which technology is being utilised in developed countries is quite different with those of third world countries. This subsequently affects the intensity of computer security. In developed countries, almost every operation is computerised, whereas in third world countries almost everything is manually processed. This concludes that to be effective in computer security, one should understand the culture of that organisation first. Questions 3 and 4 of this section therefore aimed to ascertain the culture the respondent was from so that the impact this had on their answers could be investigated.

Since this was an open survey, which means it was accessible to almost everyone who was either a member of intended discussion forum or mailing list, filtering was the only way to differentiate between experts and end-users. This was accomplished by question 5 and 6 which ascertained the respondents' background. This approach was useful during the analysis phase where the results obtained from experts were extracted and analysed separately. It was essential to separate results from experts so as to increase the reliability of the survey results. Since security experts and end-users differs in computer security understandability therefore it was important to be able to identify the opinions of those experts who know about security while being able to identify issues which may be barriers to those who are trying to learn, the end-users.

Further, question 7 and 8 aimed at further assessing the security qualifications of the respondent asking whether a respondent has any security professional qualification.

Professional qualifications are popular within the software industry. Certification programmes aim to provide an education in a set of issues where the achievement of a certification indicates that the holder is aware of these issues to a particular standard. It is therefore becoming increasingly popular. However, as was noted earlier, the need for security measures differs with the nature of organisations. In organisations A, the need for security professional qualification(s) might not be necessary but it might be a significant requirement for organisation B. So, it is necessary to determine the requirement of security professional qualification(s) so as to cover the need for including number of links for security professional bodies.

Although in some organisations, security professional qualification(s) might be a significant requirement for security role, but might not be very useful in improving computer security. Moreover, even those organisations which security professional qualification(s) is not mandatory; it might happen some of security roles have security professional qualifications. The question arise, are they going to be recognised? This explains why question 9 and 10 were included in this survey; to test the usefulness of security professional qualifications in improving organisations' computer security.

Before rushing into designing of security awareness programme, one should assess the current computer security situation of that organisation. This can be done by determining the engagement of end-users in computer security and the effort that have been put forward by that organisation on maintaining its information resources. This was accomplished by questions that fall under section two of the survey. Question 1, 4, 15, 16, 17 and 18 of this section focused on determining the effort of organisation in computer security whereas the remained questions focused on determining end-users engagement in computer security.

Although, it is very common that every organisation must have security policies in place to educate users on their roles and standards of doing their tasks, in practice this is different. The initial survey experienced this problem because it the expectation was that that every organisation operating in today's global environment would have security policies. However this proved not to be the case since in many cases, respondents most commonly in third world countries, ignored the question. This led to further investigation to find out why and it proved that it was not a valid to assume that

most organisations have some security policies. So an additional question was included in the online survey to determine whether the organisation has security policies or not so that the responses could be analysed differentiating between those respondents who worked in organisations with existing policies and those without.

Apart from Systems Administrators, there are some roles in organisation that require computer systems' administrative privileges to accomplish their tasks. Therefore, it is essential to determine what these roles are and whether they need special treatments in security awareness programme. Security policy alone would not be effective if this proved to be the case. Holders of such roles need to be educated on how to hygienically handle their privileges, like not to stay online where unnecessary and to avoid installation of applications without knowing their source. This explains why question 3 and 4 were included in the survey.

As it was mentioned previously, security policy defines computer security requirements and security awareness programme(s) informs users about those requirements and provide them with necessary skills to accomplish them. Therefore, through security policy adherence, current organisation's status of computer security and the successfulness of security awareness programme(s) can be determined. Question 15 and 16 attempted to determine this.

Security policies do change. A policy might be useful today but might not be useful tomorrow. Therefore, evaluating users' adherence alone it is not enough measurement for the success of information security. This emphasises the necessity of measuring the effectiveness of security policies. However, this contradicts with organisation's rewarding schemes. In some organisation, information security is achieved not because of security policies but due to motivation of the individuals involved. Question 17 and 18 attempted to ascertain information to allow these parameters to be explored.

6.5 Survey Results Analysis

After completion of the survey, both offline and online, the process followed was survey data analysis. From the data obtained, many interest findings were discovered. This section describes the analysis process undertaken, presenting the results of the

survey and the analysis undertaken. Only results from questions that contribute to the development of the framework will be described.

Although the structure of offline and online questionnaires differ, the online structure will be used as a guideline for the description of the analysis process. This section is divided into four phases; ICITST seminar's analysis, Tanzanian's analysis, Online analysis and combination of all surveys. Experts are expected to be more knowledgeable in the area. Conducting their results' analysis separately could have much contribution to the framework development. To accomplish this, question 5 and 6 of section 1 will be used.

6.5.1 ICITST Seminar survey results

In this survey, 30 copies of questionnaire were distributed during the registration session of the ICITST conference. Respondents were given freedom to complete the questionnaire at their convenience during the conference which lasted for four days. This survey was not so successful as compared to the one done in Tanzania. Until the final day of the seminar, only eight copies were returned which summed up to a total of 27%. However, since majority of attendants were security experts, the results obtained are still of valuable.

- ***Respondents based on country***

From the analysis conducted based on question 3 of section 1, majority of respondents were from Ireland, United Kingdom and Jordan each with 25% respondent rate. Other countries include Netherlands and United States of America with 12.5% respondent rate. These respondents were very useful, not only because they are experts in the area, but also they represent developed countries that are more advanced in technology.

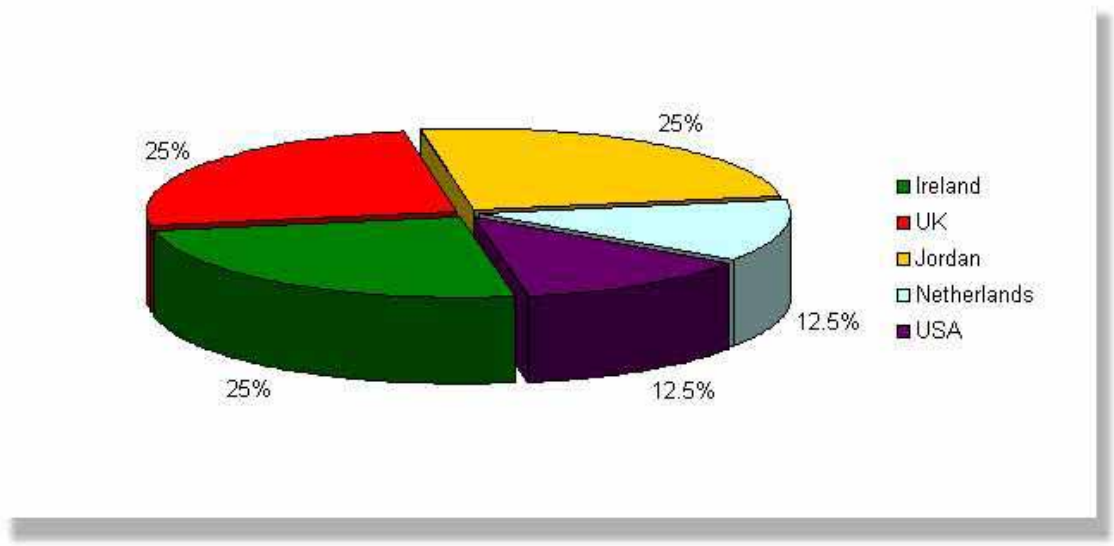

Figure 14: Distribution of Respondent based on Country

Although there were many categories of roles, all respondents opted for "Other IT Personnel" because there was no role for "Computer/IT Researcher". However, their results were still valuable because majority of them are researchers in the field of computer and information security. This was the weakness that was encountered in the offline survey but it was fixed in the online survey by including the "Computer/IT Researcher" role category in the option.

- ***Security awareness programme approaches***

The analysis of question 2 of section 3 reveals that majority of organisations with a total of 40% engage the use of email as their means of sharing information about security relevant issues. "Face-to-face" and "Presentation" approaches follow with 20% less from "Email" approach. Other approaches include "Web-based" and "Poster" with 6.7% approaches.

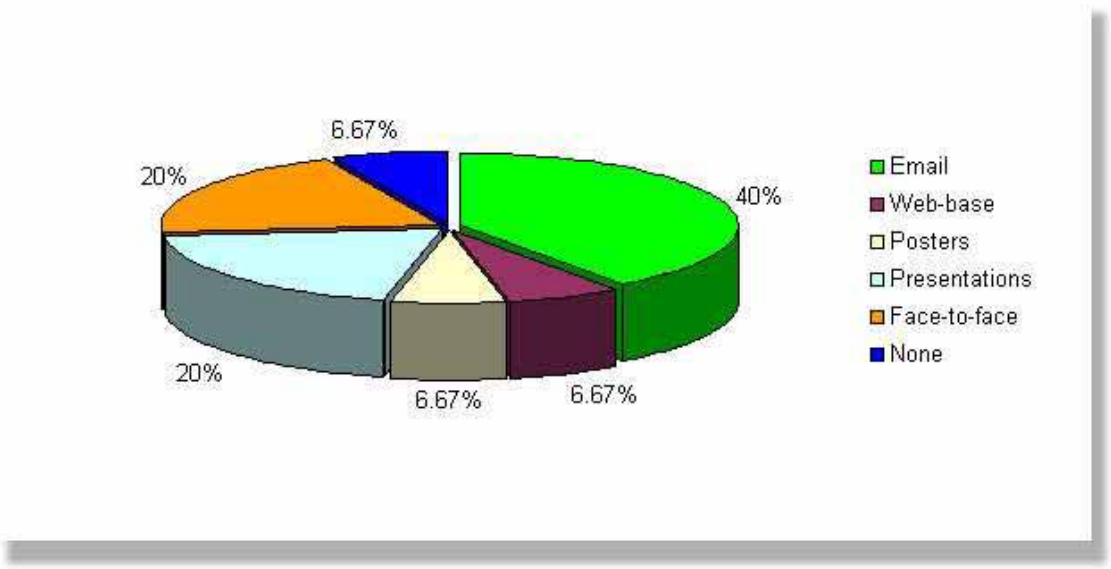

Figure 15: Distribution of Awareness approaches

However, this contradicts with an industrial opinion about the use of email as the way of communicating sensitive information (http://kmjeff.blogspot.com/). Apart from the fact that humans tends to ignore emails, especially from officemates, email tends to be so meshed up when there are many senders. When inbox is full it is difficulty to search through all the emails just to look for one particular email. Moreover, it is difficulty to track the progress of security awareness programme.

- ***Breadth of awareness programme***

The analysis of question 3 and 4 of section 3 shows that majority of respondents do not know whether their security awareness programme goes beyond the awareness of security policies. Only 28.57% of respondents were confident about their security awareness programme did go beyond the awareness of policies. Interestingly, even an experienced respondent with 6 – 9 years range of experience, and CISM and CISSP security professional qualifications, opted for a "No" option.

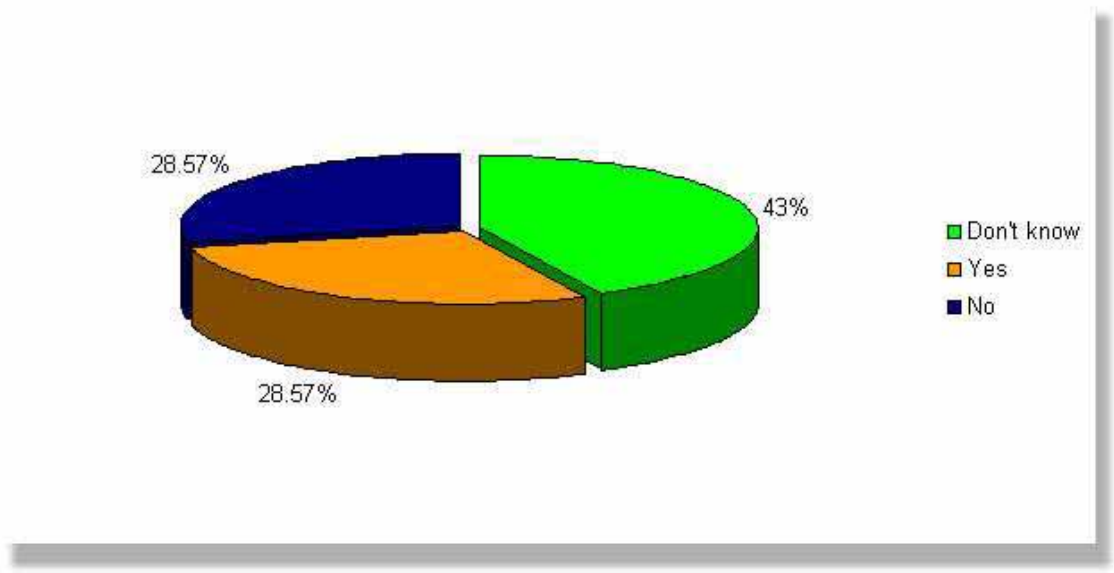

Figure 16: Breadth of Security Awareness Programme

This concludes that majority of organisations do not consider awareness programme(s) as the tool for educating users on computer security threats instead they consider it as the tool for informing users about organisational security policies.

Summarising the findings from this analysis, majority of organisations considers email facility as effective means of communicating and sharing information concerning security requirements. Moreover, their perceptions on security awareness programme are limited to security policies and not as the tool for educating users about the trend of computer threats and how to combat against them.

6.5.2 Tanzanian's survey results

In this survey 50 copies of questionnaires were distributed in education, government agencies, telecommunications and financial organisations. The survey lasted for one week from the distribution date. It was a very successful because out of 50 copies, 32 copies of completed questionnaires were collected which accounted to 64% of the whole survey results. Only 3 copies of questionnaires were damaged due to concept misunderstood, hence total percentage of survey results remained to be 58%.

However, the results obtained were quiet different with the results obtained in the previous analysis. The results revealed a huge gap of computer security perception between developed and developing countries. Therefore, the survey was extended to

include Kenya and Uganda to investigate how developing countries perceive the issue of information systems and computer security. Though it turned out their information security perception differs with developed countries, the results obtained contributed a lot in this project. It raised the issue of technological maturity to be thought when preparing awareness program which was not considered previously.

- ***Information security roles and experience***

The analysis of question 5 and 6 reveals that majority of respondents fall under 1 to 5 years category with a very little exception of 6 to 9 and 10 to 15 years categories. Moreover, majority of respondents opted for "Other IT Personnel" role category, with only six respondents on "Systems Administrator" role and one respondent on each of the remaining roles. However, this implies that majority of respondents were not necessarily experienced in computer security since "Other IT Personnel" might include any other roles like help desk, software developers, graphic designers and many alike. This is the same problem experienced in the previous survey.

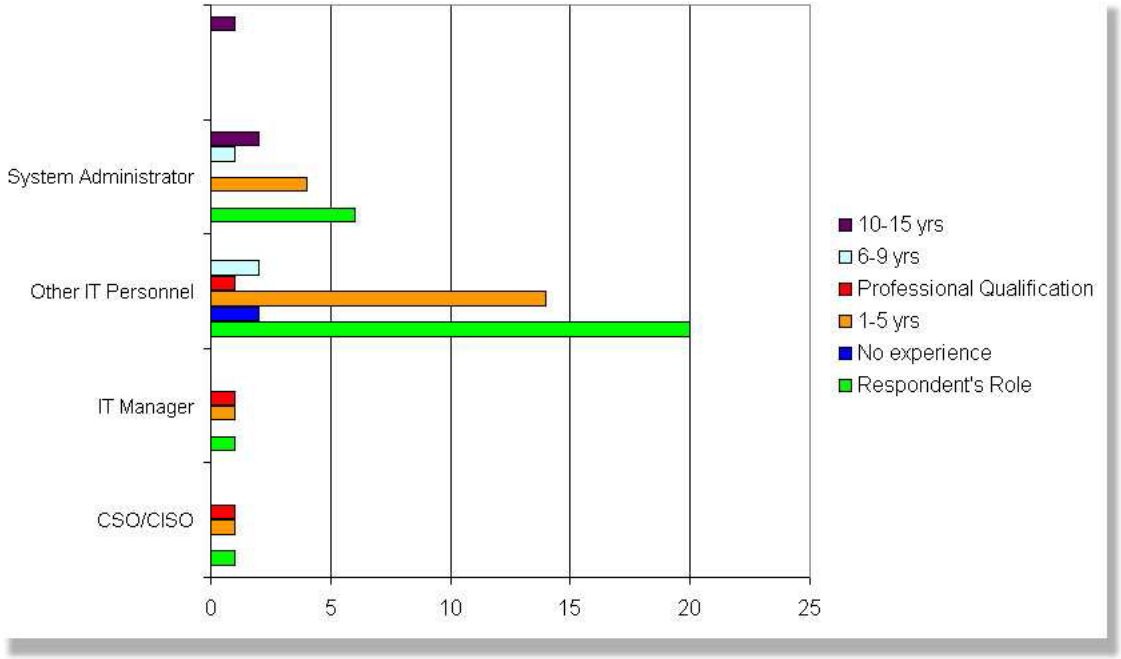

Figure 17: Respondents' experience based on role and qualification

These results could be completely different if the question was to ask for specific computer security roles without including "Other IT Personnel" role category, or to ask the respondents if they were familiar with computer security prior to answering this

question. This indicates the deficiencies of this survey that need to be addressed when designing other survey of this nature.

Nevertheless, an interesting finding can be obtained from the distribution of security professional qualifications. Although majority of respondents fall under "Other IT Personnel" category, only one respondent, who happened to be IT Security Supervisor, had security professional qualification. With remained two security professional qualifications to "IT Manager" and "CSO/CISO" categories. Moreover, only one respondent opted for "CSO/CISO" category with none in "CIO/CTO" category. This concludes that computer security in Tanzania has not yet been considered as an issue.

- ***Users' involvement with computer systems***

Moreover, analysis was done to determine the use of computer systems in Tanzania. Based on question 1 of section 1 and question 3 of section 2, it was discovered that majority of organisations involve their employees in using computer systems with 44% "High" and "Medium" categories . This can be graphically represented in figure below. However, this should not be confused with technological maturity of organisations. Majority of organisations in Tanzania are still operating manual. They use computers for office operations like report writing and very simple applications.

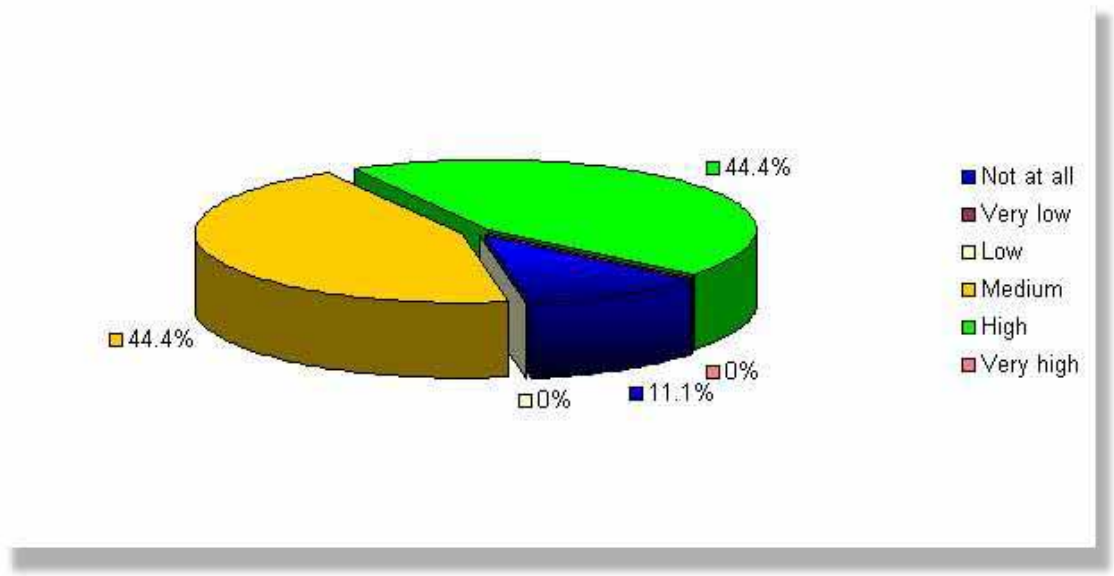

Figure 18: Distribution of end-users in operating computer systems

Contrary, the results could be completely different if the question asked the number of operational information systems and/or their rate of connectivity to internet. Tanzania is still in automation level of technology. Based on an informal pilot survey, banking and telecommunications industry are termed to be the most successful in technology. However, there is no any transaction which are performed online except for balance enquires. These results have affinity with the results obtained by a telecommunications survey conducted by International Telecommunications Union (ITU 2007). Their result revealed that Africa has 2.5% internet subscribers compared to other continents such as Europe with 29%.

- ***Applicable security awareness approaches***

The analysis of question 2 of section 3 shows that email, presentation and web-based are the common forms of awareness programmes with email as the highest with 43%. Thereafter it follows "Presentation" with 23% and the third approach is web-based with 20%. Other approaches include "Face-to-face" with 8%, "Posters" with 5% and 3% without security awareness programme at all.

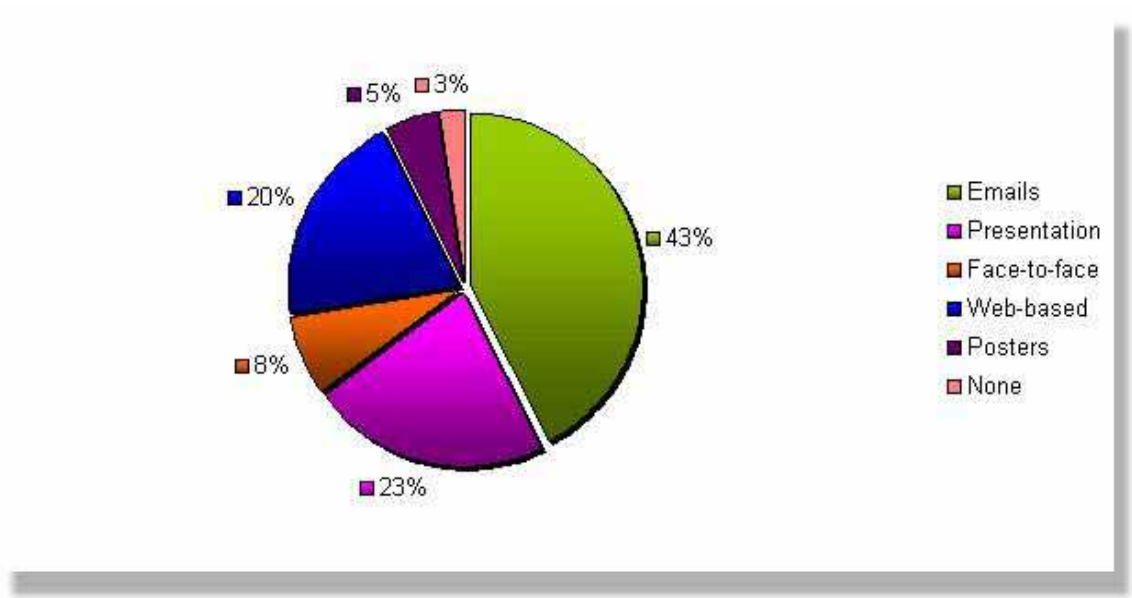

Figure 19: Distributions for security awareness approaches

However, the results could be completely different if an option of "Not Applicable" was included. This is because the most common query posed by respondents was what was meant by security user awareness programme. This implies that majority of respondents chose "email", "web-based" and "presentation" approaches because there

were common terms to them. Another interesting finding is the 3% of "none" option. This again emphasises the low maturity of information security in Tanzania.

- ***Information security perception***

The analysis on question 1, 2 and 3 of section 1 against of that of question 1 of section 2 reveals that the issue of computer security in Tanzania is very far behind hence many organisations does not take it as a serious issue. The results represented in the graph below shows the distribution of security professional certifications in different organisation.

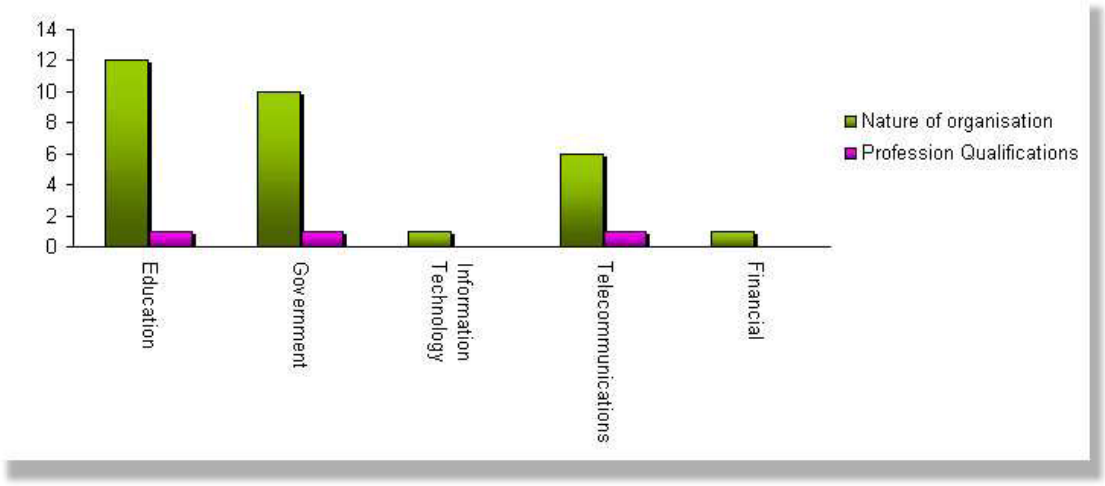

Figure 20: Distribution of Security Professional Qualifications in Organisations

Only three respondents from government, education and telecommunication have security professional qualifications. Moreover, as it was shown in Figure 17, only one respondent have security role i.e. "CSO/CISO". This concludes that many organisation in Tanzania they does not see the potential of information security.

Findings obtained from this survey, triggered a pilot survey to other developing countries including Kenya and Uganda. These countries were picked because they are near to Tanzania and more importantly they present a clear picture of developing countries. Due to time limit, the approach employed was to contact key personnel in computing department of different organisation and ask general questions based on the results obtained from Tanzania.

Surprisingly, the answers received were very much in line with the results obtained from Tanzania. This again aroused curiosity for finding what reasons are behind this. Furthermore, another survey was conducted. The approach was to browse different universities' web pages searching for modules that teach students on information systems security. The survey discovered that only few universities teach modules similar to information security. The majority of these courses are offered in training centres which is a bit expensive for an average person.

6.5.3 Online survey results

The aim of this project was to develop a framework that will leverage KMS to improve security awareness. It is clear from the aim that this framework is not a closed framework tightly to a specific country and/or organisation. Therefore all possible input must be considered prior to its designing. To accomplish this, the questionnaire was posted online so as to gain different views from different countries all over the world. The survey had large input to the project because many of the audience who responded are security researchers and experts from different countries.

The survey lasted for three weeks period. 111 respondents responded to the survey and 43 of questionnaires were fully completed with 22 respondents who did not replied at all. The survey was very successful because the response rate was very high with many countries which are regarded as benchmark for information security. Country like USA which is second high in the chart is far away in information security. Therefore from this huge number of response, useful information can be obtained.

- ***Respondents by country***

The analysis of respondent based on countries as shown in Figure 21, the top three countries are Tanzania with 22.6% followed by United States of America with 20.2% and 14.3% for United Kingdom. Other countries which are in top five include Ireland with 13.1%, and Malaysia and Singapore with 3.6%. The remaining countries which also participated in the survey include Sweden, Switzerland, Venezuela, Indonesia, Iceland, Pakistan, France, India, Singapore, Mexico and Romania, Germany, Nigeria, China, Hong Kong, Canada and Portugal.

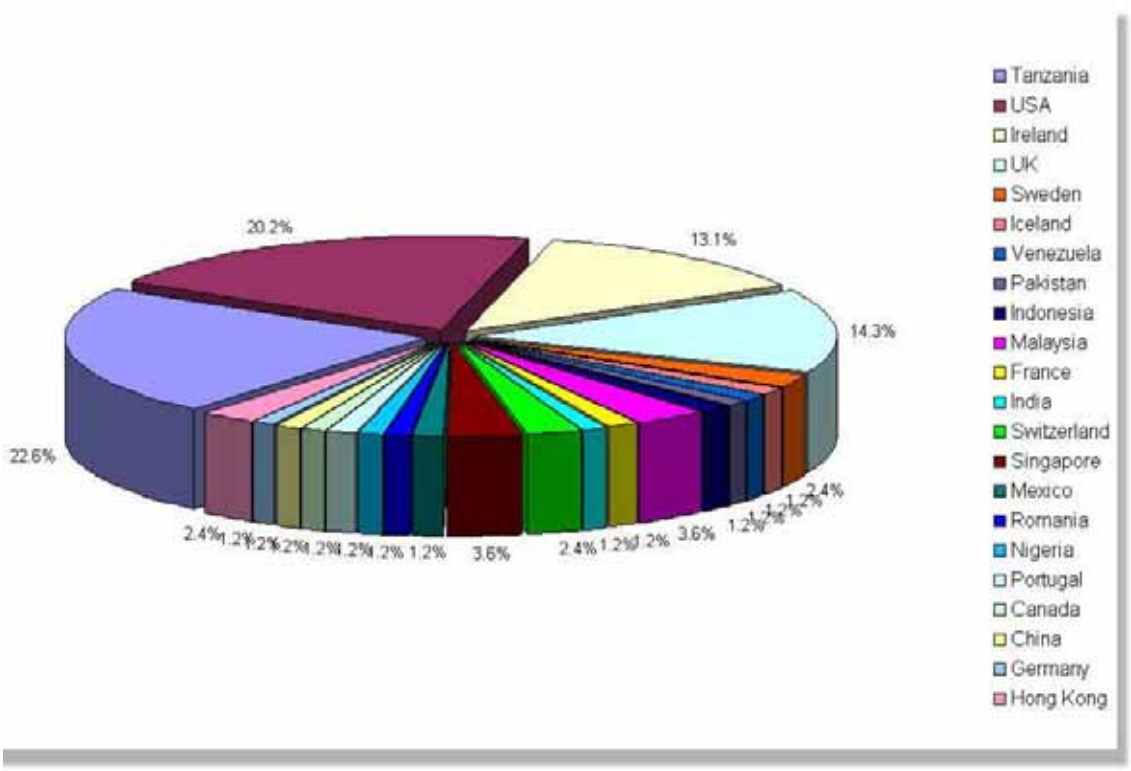

Figure 21: Respondents by country

As shown in the chart, many countries participated in the survey. This shows the reliability of the results and hence provides good inputs for the design of the framework which is the objective of this project. Besides the reliability of the results, the survey also proves to be interesting to win such a huge number of respondents in a very short period.

- ***Users' involvement***

The analysis of question 2 of section 2 reveals that majority of organisation ignores users' involvement in establishing security policies. As shown in Figure 22, majority of respondents agreed opted for "Medium" category with 26.8% then followed by 24.4% of "Very low". On the other hand, only few of respondents opted for "Very high" and "High" categories with only 4.9% while others opted for "Low", "Very low" and "Don't know" categories with 17.1%, 14.6% and 7.3% respectively. Statistically, only 36.6% of respondents consider users' involvement in establishing security policies. Therefore, 65.4% of respondents they either take it for granted or do not consider it at all.

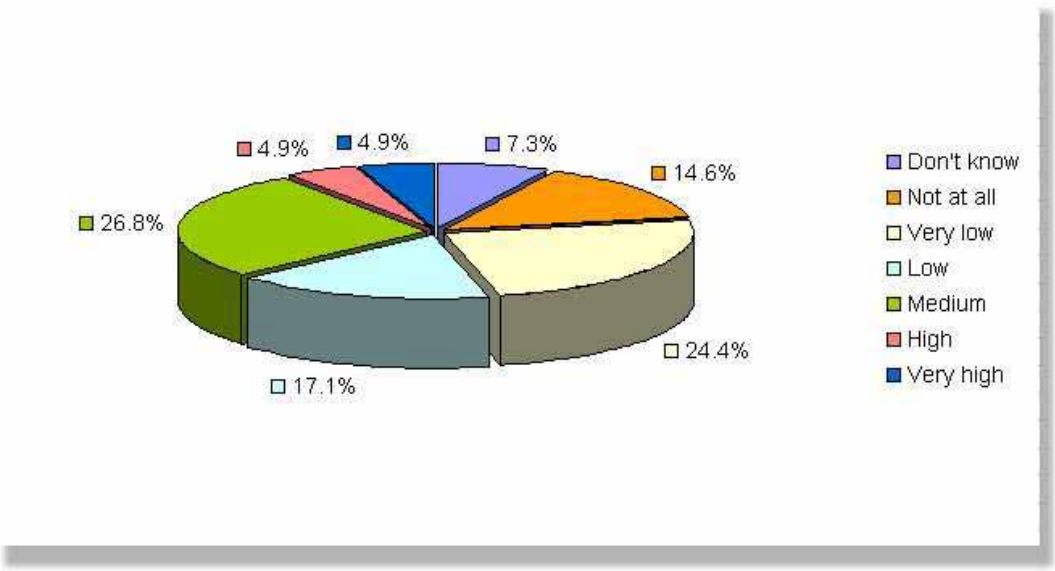

Figure 22: Users' Involvement in Policy Establishment

- ***Security adherence***

Users' involvement in security policy establishment is directly proportional to their adherence. As the shown in Figure 23 the values for users' involvement during security policy establishment is directly proportional to the values for security policy adherence. Therefore, this emphasises that users' involvement in security policy establishment determines their adherence with security policies.

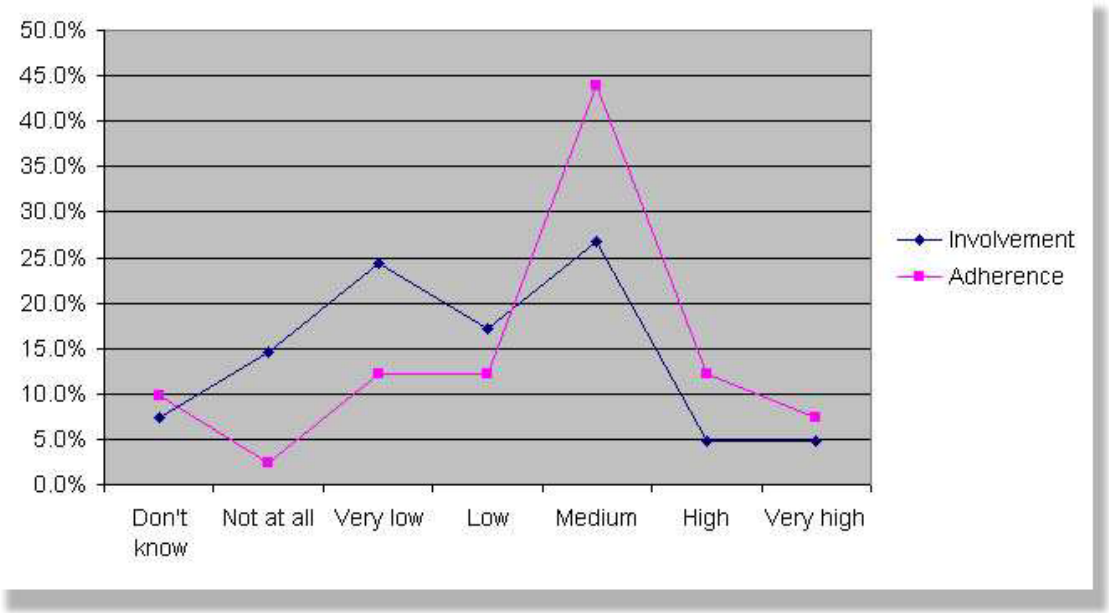

Figure 23: Relationship between users' involvement and policy adherence

6.5.4 General survey results

The previous analysis focused on analysis of individual surveys. However, since the aim of the survey was to investigate the roles users play in computer security and the effect of security awareness programme in educating users, it is now plausible to combine the results from each survey and analyse so as to gain the general results.

- ***Poor user involvement in security decisions***

As previously results revealed, user involvement in security relevant decisions is very poor. The analysis was done based on the question asking if the respondent's organisation considers users in establishing security policies. As shown in figure 24, majority of respondent are between "Medium" and "Low" categories, with only total of 8% of "High" categories. On the other hand, as shown on graph (b), users' involvement is directly proportion to their adherence with security policies. This concludes that majority of organisations involved in the survey does not consider users' participation in security related decisions and thus it has impact on the successful of organisational computer security.

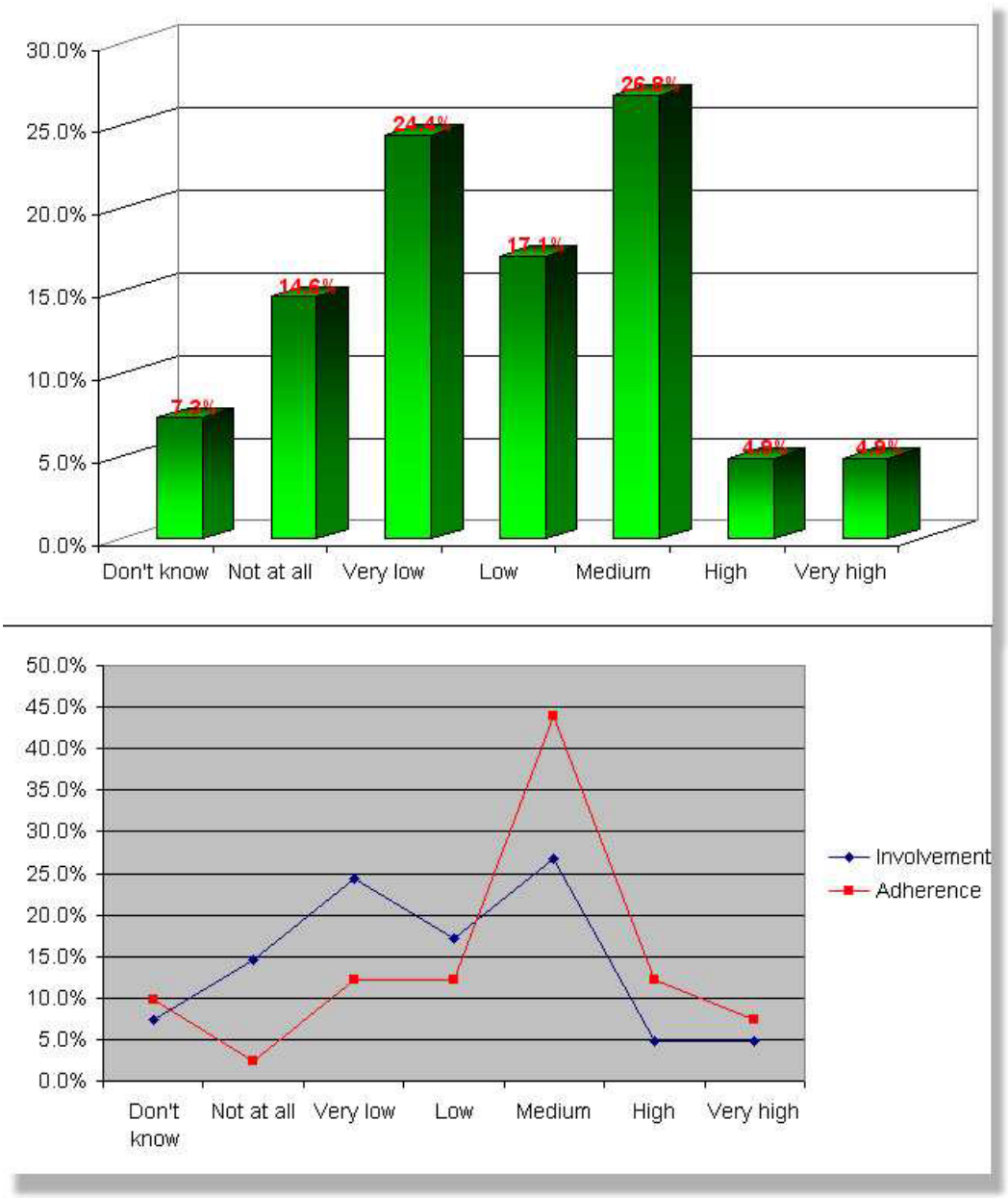

Figure 24: User involvement in security decisions

- ***Computer security perception***

Comparison of survey results from Tanzania and those collected from ICITST revealed the difference in computer security perceptions between developing and developed countries. The results revealed that Tanzania which represents developing countries is very poor in understanding computer security. As it is shown in figure 25, the comparison of security qualifications, roles and government involvement between developing and developed countries revealed there is a gap of 1:3 ratios in computer security. The results show the respondents from developing countries have only 4

security qualifications out of 48 respondents, inclusive 19 respondents from online survey. On the other hand, developed countries have 12 security qualifications out of 65. Moreover, comparison of government involvement in security issues reveals the gap between developing and developed countries. As shown in figure 25, government involvement in computer security is poor compared with developing countries.

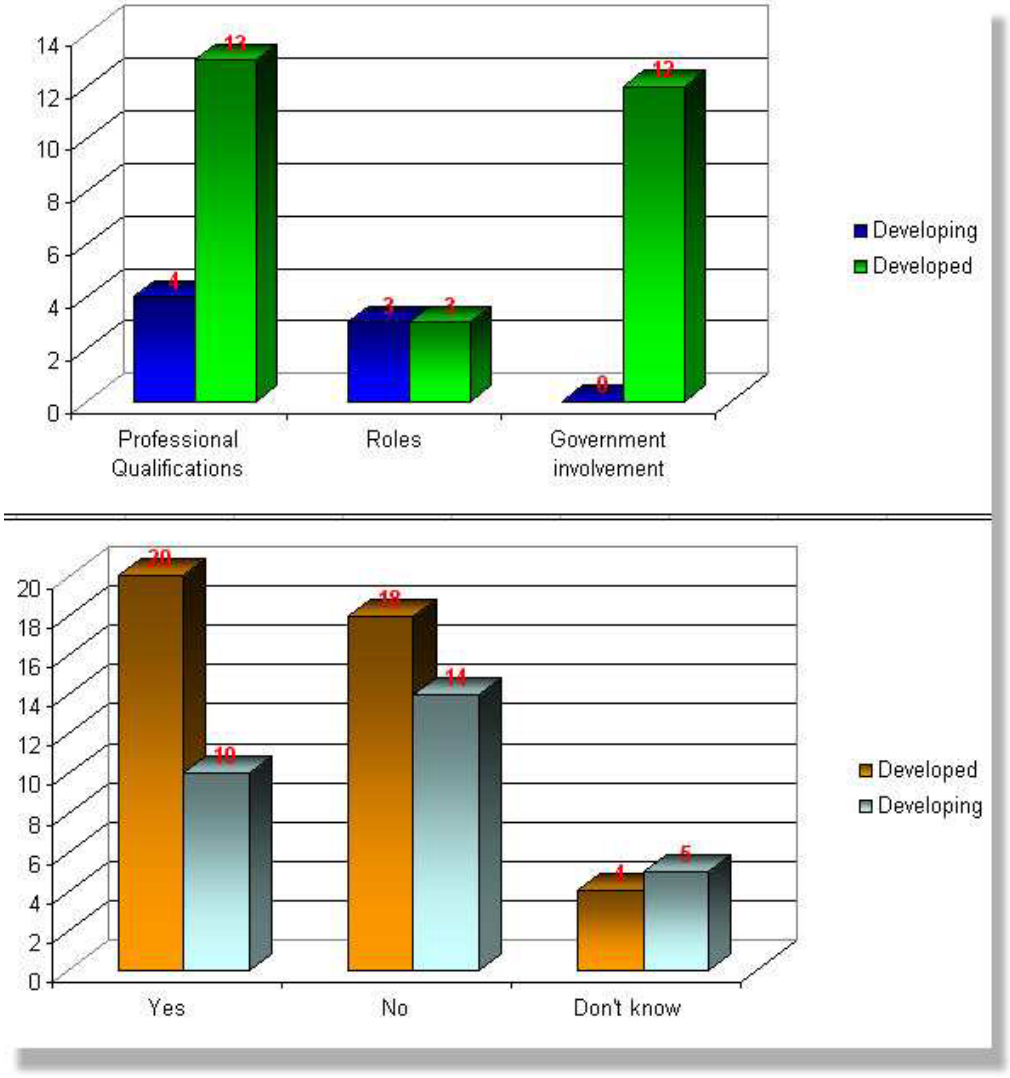

Figure 25: The gap of computer security between developed and developing countries

Moreover, based on the question that was asking respondents about whether there is security awareness programme in their organisations, results confirm the gap between developed and developing countries. The gap between "Yes" from respondents from developed countries is twice as the response from developing countries. Moreover, the number of respondents who did not know whether there is security awareness programme in place is high for developing counties compared to developed countries.

- ***Email as a major tool***

Both the results from all surveys show that email is a leading approach for security awareness programme. As shown in the figure 26, for general results email is the leading approach followed by web-based which is 8.09% less than email approach.

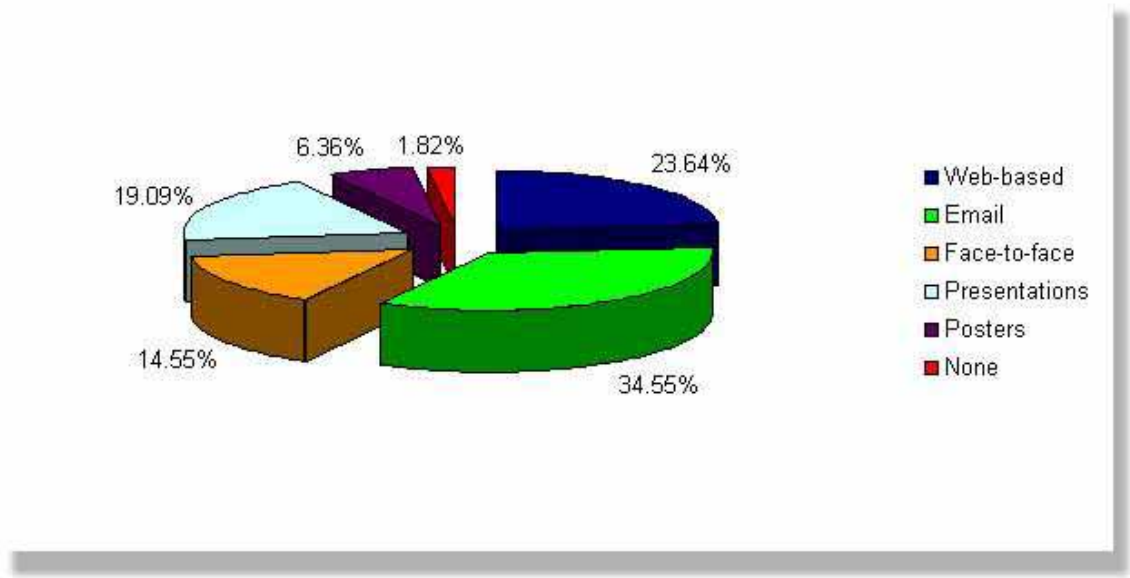

Figure 26: Distribution of security awareness approaches

- ***Narrowness of security awareness programme(s)***

The analysis was done based on the question asking whether security awareness programme(s) goes beyond the awareness of security policies. As it can be seen from the diagram 27, majority of respondents opted for "Yes" with 49.18% followed by "No" option with 36.07% and finally with "Don't know" with 15%. However, thought the results shows majority of organisations consider awareness programmes to go further, but in totality the result is poor because it is only 49.18% of the whole results. This concludes that security awareness has not yet been seriously practiced.

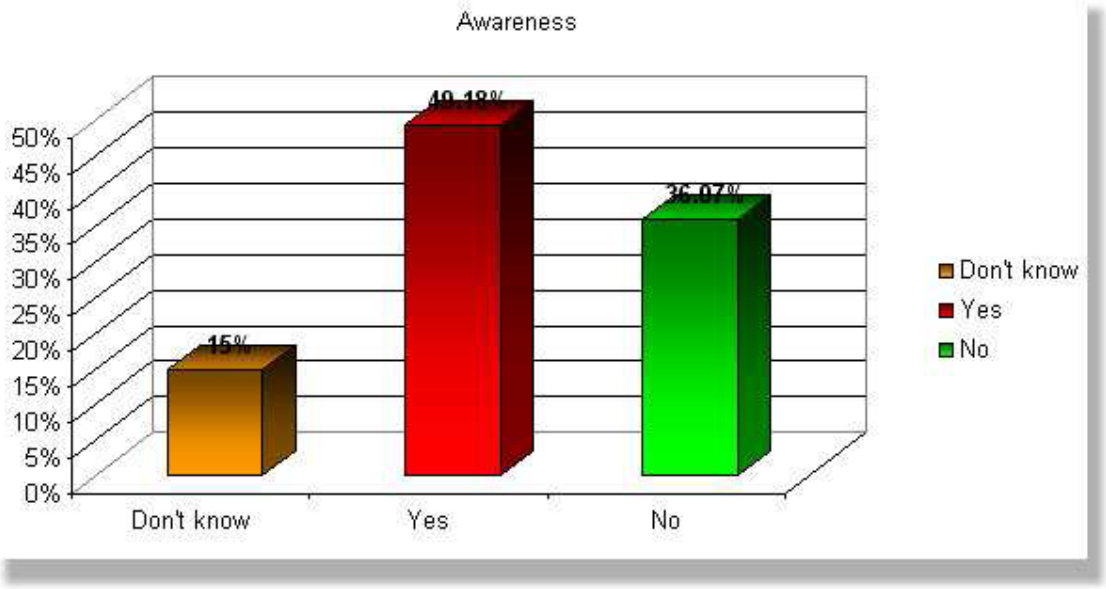

Figure 27: Breadth of Awareness Programmes

6.6 Supporting interviews

6.6.1 Interview design

The aim of this survey was to investigate the roles users play in computer security and the effort of the current security awareness programme into educating users in security related issues. The survey was successful with reasonable number of participants whom majority were security experts. Many findings were obtained. However, since these are the inputs for the development of the framework, therefore it is plausible to evaluate them prior to their applicability. Therefore, the primary aim of these interviews was to evaluate findings as obtained from both literature review and the survey as well.

The questions of the interview were derived from findings both from literature review and survey. Six questions were derived, each covered findings from both literature review and survey. A complete structure of interview is provided in appendix B. The interview questions were then tested for completion time by imitating the interview session with colleague. The resulted completion time was 45 minutes.

6.6.2 Interviewee contributions

- ***1st Interviewee***

The interview was conducted on August 25th 2008 with a former security expert in computer security which lasted for one hour. To be in the same line with interview questions, the interview began with briefly explanation of the project aim. Thereafter, the interviewee initiated a general discussion of the structure of the interview questions where some comments were noted. After a general discussion of interview questions, the main theme of the discussion was initiated where the interviewee commented in a number of things both general for the dissertation and specific for interview session.

The initial comments which were noted were based on the look and feel of interview questions. Among these comments was the generic nature of the interview questions. The interviewee commented that the questions are too general and they should focus on specific issue. For instance in question one, the interviewee noted that the question did not state what type of users the question is focusing on. Furthermore, the interviewee commented on the clarity of the questions and suggested for inclusion of examples to give a clear picture of questions. For instance in question 1 and 2, interviewee suggested including examples of policy and topic of material respectively.

Following the interview theme, in question 1 and 2, interviewee agreed with argument but with exceptions that only the management and/or IT personnel who participate in policy making and/or security awareness building process, respectively, should be the last decision makers. The interviewee commented that there are negotiatable and non-negotiatable security policies. For non-negotiatable security policies users must be told and follow while negotiatable users can discuss about the establishment of the policy.

However, in Knowledge Management context the author believe that regardless of the nature of the policy, employees' engagement in establishing security policies is essential for its success. This is because employees will feel a sense of being respected and not just dragged like machine. This will make the employees to have trust with their management and thus motivates them on opening up for new idea.

"Engagement communicates management's respect for individuals and their ideas."
(Kim & Mauborgne 2003)

Proceeding with the interview, in question 3 and 5 the interviewee also agreed with the argument that both organisational culture and security culture are crucial factors to be considered. However, the interviewee argued that these cultural factors go *head-to-head* with domain of the organisation. Therefore, a clear understanding of the domain determines the cultural behaviours of the organisation. This comment was inline with author's view.

In the general comments of the dissertation, interviewee commented on the clarity of the dissertation where further emphasises were on the scope and relevance of literature review and definitions of factors.

6.7 Summary of findings

6.7.1 Poor user involvement in security decisions

The analysis shows, see figure 24, that users involvement in security policy establishment is poor and thus it has direct impact on users' adherence with security policies. Therefore, this reveals that if users could be involved in security related decisions, security policy compliance could increase and hence increase in computer security in general.

6.7.2 Computer security perceptions

The analysis of the results from both surveys reveals a gap of computer security perception between developing and developed countries, see figure 25. This is apparently because of differences technological infrastructure maturity. Unlike in developed countries, majority of organisations in developing countries are still operating manually (Bugada 2005). Therefore, this will subsequently reduce computer threats and hence its consciousness.

6.7.3 E-mail as a major security awareness approach

The survey reveals that e-mail has dominate as a major channel for disseminating security awareness materials with a little exception on web-based approach, see figure 26. This explains why majority of security awareness programme fails. This is because email is not a convenient tool for facilitating collaboration.

6.7.4 Narrowness of awareness programme(s)

The survey results reveals that majority of organisations does not consider awareness as a broad means of educating their employees on security issues more than security policies, see figure 27. This explains why the number of security break-ins increases.

6.8 Conclusion

This chapter aimed at describing security awareness survey. In section two, explanation of survey audiences was conducted which included both security experts and end-users. The survey was based on both online and physical distribution of questionnaires. In physical distribution, questionnaires were distributed in ICITST seminar which was held in Dublin Institute of Technology and in Tanzania. The results obtained from questionnaires distributed in Tanzania triggered the extension of the survey to other developing countries including Kenya and Uganda.

The description of survey designing was conducted in section four where the aim of each question was explained. The analysis of survey results was conducted in section five where each survey was separately analysed and finally combined. Among the findings of the survey is the gap of security perception between developed and developing countries. Other findings include poor users' involvement, dominance of e-mail in security awareness, and the shallowness of security awareness programmes. The following chapter describes the development of a framework and prototype implementation.

7 KMS-SAWA FRAMEWORK AND PROTOTYPE IMPLEMENTATION

7.1 Introduction

All the way from chapter 2 of this dissertation to chapter 5, the research presented has been focused on establishing the foundations for the heart of the project described in this dissertation which is to investigate how KMS could be useful in improving security awareness in an organisation context. From the research documented in previous chapters, a framework to use KMS to improve security awareness has been developed that leverages the findings obtained. This chapter discusses the development of this framework.

The chapter starts by discussing key factors which were found to influence the creation of a KMS to support security awareness. Further the chapter extends the findings not just to the development of a KMS but to the development of a security awareness programme in any form. The chapter discusses the iterative development of KMS-SAWA framework. The chapter then moves on to discuss the implementation of a prototype KMS for security awareness using Wiki technology and concludes by presenting the evaluation of this prototype and drawing conclusions on the overall usefulness of the premise of the project described in this dissertation .

7.2 Factors for KMS implementation for security awareness

In this dissertation the determination of organisation's technological maturity, security culture, and organisational culture have been identified as crucial factors for successful implementation of KMS for security awareness programme. This section focuses on discussing each of these factors by going into details on determining the criterion for their categorisation.

7.2.1 Technological maturity

From the findings obtained from the survey results, it is clear that technological maturity of an organisation determines the consciousness of computer security.

Technological maturity defines the advancement in computer technology in an organisation or any area where it is applicable. The survey results revealed the gap of computer security perceptions between developed and developing countries. Therefore, since the framework is an open framework, it is plausible to determine the technological maturity of the organisation prior to building process of security awareness programme.

Most of previous approaches overlooked the necessity of determining the technological advancement of an organisation with the assumption that all organisations are well established in technology. However, this is not the picture of third world countries. As it was noted previously, in third world countries, computers are mainly used for office operations with limited internet access for communications purposes. Although there are few organisations such as financial institutes, government and telecommunications which are said to be advanced in technology, but still many of their tasks are manual carried.

However the challenge remains on how to determine organisation's technological maturity level. Fortunately, this process can be carried out just like requirements analysis phase of software development life cycle. Therefore, normal techniques for data collection, such as interview, observation, survey and many alike, can be applied in this phase and come up with useful information. However, the problem still persists, after obtaining for instance the number of applications that are operational and their categories, how can someone categorise between high and low technological maturities?

By itself, developing a criterion for determining the level of technological maturity in organisations is enough title for the MSc. Dissertation. It requires an extensive research on how different organisations perceive the potentiality of computer applications in hand and how should they categorise applications based on their usability. Therefore, for the purpose of this dissertation this issue will be ignored and considered as a future work for this project.

7.2.2 Organisational security culture

Understanding the level of technological maturity provides a clear picture of computer security perceptions of an organisation. However, the analysis of organisational security culture is crucial prior to the implementation of KMS for security awareness programme. Organisational security culture defines organisation's initiatives toward computer security. These initiatives include encouragement of security collaboration events, motivation schemes for practicing good security principles and users' engagement in security related decisions. The survey results shows majority of security awareness programmes fail because they ignore the cultural component. It is illusion to deal with human elements without considering their intuitions.

However, the challenge here is not on how to measure the level of security culture within organisation, the challenge is on how to measure their successfulness. What is interested in this factor is on how current security initiatives help in minimising computer threats and not how many initiatives are currently running. It is possible to have many security initiatives but with poor results in computer security, which is the focal point for their existence. Therefore it is crucial to determine how effective these initiatives are prior to building awareness programme.

The level of organisational security culture can be measured by quantifying current security initiatives of the organisation. Contrary, the effectiveness of security culture can be measured by the number of computer security break-ins before and after the initiation of the initiative. The decrease of computer security break-ins indicates the successfulness of security culture and vice-versa. Therefore, the higher the decrease rate of security break-ins the higher successful of initiatives so is the higher the level of security culture and vice versa.

7.2.3 Organisational culture

The organisation's technological maturity level and organisational security culture determines the level of implementing security awareness programme. However, explanation of the level of security awareness programme implementation is beyond the scope of this section. This section only focuses on the description of organisational culture in successful implementation of KMS for security awareness programme. This

factor is in line with the first phase of building security awareness programme as explained in chapter 3. In this context, organisational culture defined by the rules, procedures, standards, values and mode of conduct of organisation's operations.

As it was explained in chapter 4, understanding the nature of organisation is crucial in determining the type of KMS to be implemented within the organisation. The production type of an organisation with its market flexibility determines the type of KMS to be implemented. Moreover, Desman (2002, pp.19-25) emphasises on understanding the means of communications that are appropriate and applicable for both the management and subordinates within the organisation. Therefore, all these emphasise the necessity of understanding the culture that drives an organisation. However, this is not about measuring its effectiveness or contributions in computer security. This factor is for determining the "do's" and "don'ts" of organisation. Therefore, for determining the type of KMS to be deployed to a specific organisation, a product-service model as described in chapter 4 will be used.

7.3 Initial KMS-SAWA framework

As mentioned previously, for an organisation to successfully leverage KMS to improve security awareness programme it needs to fulfil three factors; *technological maturity*, *organisational security culture* and *organisational culture*. Technological maturity factor determines the level of computer security perception whereas organisational security culture determines the initiatives for computer security improvement. Organisational culture determines the "do's" and "don'ts" of the organisation.

The first two factors, *technological maturity* and *security culture*, acts as active factors where they must be fulfilled for organisation to initiate security awareness implementation process. Depending on their fulfilment, these factors determine the implementation level of security awareness programme. On the other hand, the final factor which is *organisational culture* determines the type of KMS to be implemented for disseminating security related materials. However, since the framework will be practically used, it was worthwhile to be evaluated by security experts (evaluator).

Therefore, this section focuses on describing the evaluation process of the framework. However, it should be noted this evaluation is just an initial evaluation focusing only on the framework readability and applicability to the organisational context. Another evaluation which will focus on usability of the framework will be explained in section 7.5. This evaluation session was based on oral interview where the author met face-to-face with evaluator. The session started by briefly explanation of the framework and how it intended to function. After the explanation, evaluator commented on some of issues.

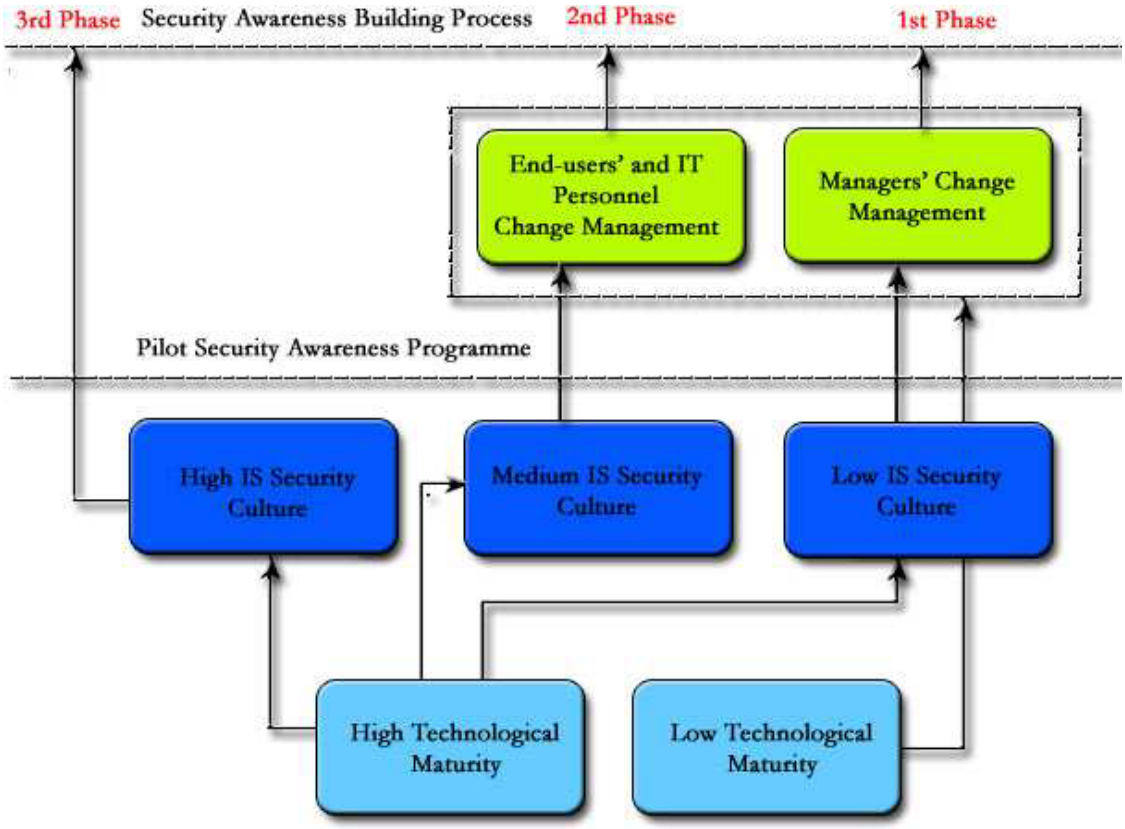

Figure 28: Initial KMS-SAWA Framework

As shown in figure 28, the framework, as notified by *evaluator*, lacks the correlation between the implementation phases. That is, there is no a clear cut point showing the incremental implementation if the organisation falls under the 1st phase of implementation. Moreover, *evaluator* pointed out that there is no clarity on the scope of *pilot security awareness programme*. Evaluator also pointed out that the framework does not show the exemption of 3rd phase on *pilot security awareness programme*.

Furthermore, the framework does not show the third factor to be considered for the implementation of KMS for security awareness. Finally, the *evaluator* argued on the complexity of categorising cultural issue within organisations. Therefore, the *evaluator* suggested for reduction of organisational security culture into high and low categories.

On session adjourning, the *evaluator* commented on the applicability of the framework in an organisational context with the conditions to amend all the deficiencies that were identified during the session. All these comments were then worked on and are reflected in the new framework, see figure 29.

7.4 KMS-SAWA framework descriptions

As mentioned previously, pre-evaluation of KMS-SAWA framework focused on readability and applicability of the framework. Based on the comments from the *evaluator*, new framework was developed to accommodate all comments. Therefore the whole of this section will focus on describing the KMS for Security Awareness (KMS-SAWA) framework, see figure 28.

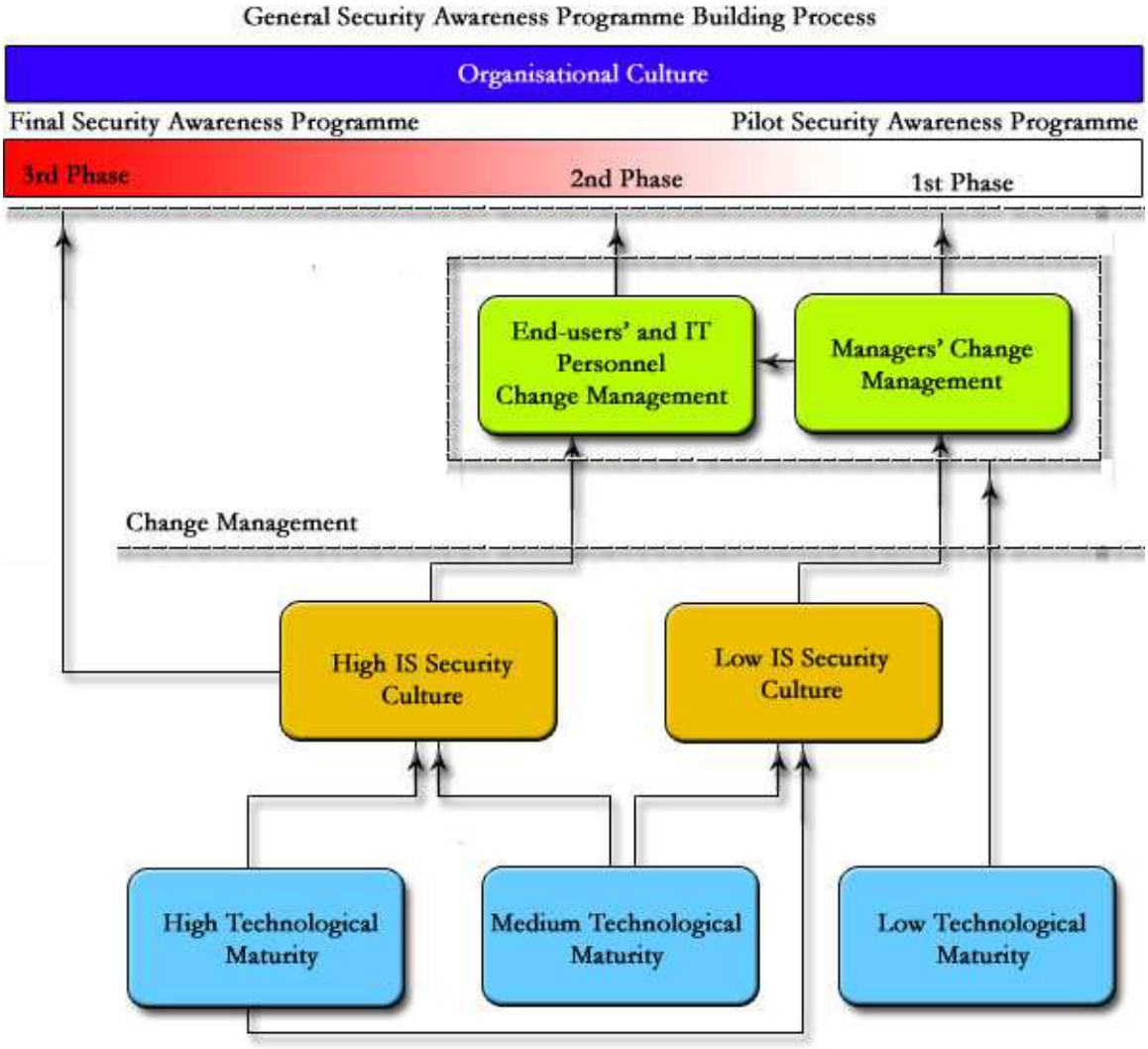

Figure 29: KMS - SAWA Framework

As it can be shown in figure 29, the framework has two layers of security awareness programme(s); middle layer which is *pilot* security awareness programme and upper layer which is the actual implementation of security awareness programme. Pilot security awareness programme is a temporary strategy to ensure security awareness within an organisation while it is in a transition period. However, this is with exceptional for 3rd phase of implementation which goes directly to initiate the permanent implementation of KMS for security awareness.

Moreover, depending on the implementation phase, organisations might require to initiate a change management programme to introduce security culture prior to actual implementation of security awareness programme (Alavi & Leidner 1999). Again depending on implementation phase, this change management may target either both

user categories; end-users, IT personnel and Managers, or only end-users and technical staff. Much detail on change management programme will be discussed in section 7.4.1 and 7.4.2.

The approach used to describe the KMS-SAWA framework is based on its implementation phases. Therefore, the 1st phase of implementation will be discussed followed by 2nd phase then finalise with the 3rd phase. All components of the framework, starting from bottom up, will be implicitly described in the descriptions of each phase. However, it should be noted that the order of implementation phases is not rigid. Depending on the levels of technological maturity and security culture of the organisation, any phase can be implemented first.

7.4.1 1st Phase of implementation

As it is shown from the framework, figure 29, organisations that have low technological maturity level fall under the first phase of implementation. As referred from the survey findings, the level of technology has impact on computer security perception and computer security in general. Therefore, building on this finding, organisations that have low technological maturity are subsequently poor in security culture. As it can be shown on the framework, organisations that fall in this category must initiate a change management programme that aims at preparing end-users, IT personnel and executives prior to the implementation of KMS for security awareness. The aim of this change management is to educate them the benefits of computer security and security culture as well so as in return they can be the champions into engineering its adoption within the organisation.

Meanwhile a pilot security awareness programme must be initiated to temporarily accommodate the needs in hand. This is the first form of security awareness programme. Security awareness programme in this phase is in its simplest form that focuses mainly on temporarily disseminating security related issues within the organisation. However, if organisation in this phase chooses to concentrate with managerial change management and ignore the other bit, then it will always remain in phase one unless it changes its status of technological maturity. Therefore, for organisation in this phase to implement KMS for security awareness must overcome

phase 1 which is basically concerns with managers' change management and thereafter to undergo users' and IT personnel change management.

Moreover, organisations that fall into a medium class of technological maturity, they will then be tested for the level of security culture. If the organisations fall in the low class of security culture, they will again fall into the first phase of implementation. However, the difference from the previous first phase is that for this phase change management programme is not as intense as the previous one. In this it is assumed that managers have insights on why computer security is essential for their business.

7.4.2 2nd Phase of implementation

The previous phase of KMS implementation focused on change management for both users and IT personnel, and managers. In the second phase of implementation, the focus is the change management for users and IT personnel. Therefore, organisations that has medium technological maturity level and high level of security culture falls under this phase. Meanwhile, the pilot security awareness programme needs to be implemented to temporarily handle the current situation of disseminating security related issues.

In this phase, a change management programme focuses on users and IT personnel. As it was discovered from the literature review, the gap between users and security personnel has impact on the successfulness of security awareness programme and computer security as well. Therefore, the aim of this change management programme is to resolve this gap that exists between security experts and users by explaining to them the importance of knowledge sharing and their impact in security of corporate information assets. Again this phase must fulfil the requirements of this phase prior to actual implementation of KMS for security awareness programme.

Moreover, all organisations that have high technological maturity level but medium security culture fall in this phase. However, change management in this is not as intense as the previous category. In this, it is assumes that the gap between end-users and security personnel is small and hence slight effort is required resolve the gap.

7.4.3 3rd Phase of implementation

If organisation has fulfilled all the requirements of phase one and two of implementation then it enters into the third phase. In this phase, the actual implementation of KMS for security awareness is initiated. As it was discovered in the literature review, organisational culture is a central for the successful of security awareness programme. Therefore, in line with this finding, prior to the implementation of KMS for security awareness, organisational culture is considered in this framework. Unlike technological maturity and security cultural factors, organisational culture is for determination of the "do's" and "don'ts" of the organisation. Therefore, after analysing cultural element of an organisation, normal process of building security awareness programme, as described in section 3.4, follows in the context of KMS.

Meanwhile, for organisation that has not pass through phase one and two, it will be tested for its technological maturity level. If the organisation fell in a high class it will then be tested for the level of security culture. Again if the level of security culture is high, then the organisation is declared to be mature enough to initiate the actual implementation of KMS for security awareness programme. Therefore, this level skips the change management phase and pilot security awareness.

7.4.4 Summary of why KMS-SAWA framework is a solution

This framework is useful in implementing KMS for implementing security awareness programme because it addresses all previously identified problems for the failure of successfulness of current security awareness programmes. From the literature review it was pointed out that user' involvement, poor material preparation and delivery, ignorance of organisational and security culture are among the reasons to why current security awareness programme fail. Moreover, survey findings also emphasised on users' involvement and consideration of computer security perceptions.

In resolving all these, the KMS-SAWA framework considers computer security perceptions and security culture by including these as factors to determine the level of change management. It is this change management that focus on resolving the gap between users and security personnel. Therefore, by resolving this gap users' involvement will definitely be increased and hence improves security awareness

material preparations. Moreover, organisational culture is considered to resolve any conflicts with organisation interests so as to define appropriate type of KMS to facilitate security knowledge sharing between members of all levels. Therefore, by deciding on the appropriate KMS for disseminating security awareness material, greater response from users from all levels of management will be attracted.

7.5 Prototype implementation

As it was described in KMS-SAWA framework, for a successful implementation of KMS on security awareness context, three phases of implementation must be accomplished. However, this only depends on the level of technological maturity and security culture of the organisation. Moreover, organisation type and the number of users also determine the nature of KMS to be implemented for that particular organisation.

This prototype was implemented to operate within any education institution with the main concentration to lecturers as users. For the purpose of demonstration, this prototype concentrated with the final phase of implementation with the assumption that the underlying organisation is stable both in technology and security culture. Therefore, effort is on disseminating security relevant material. Furthermore, due to time limit and complexity nature of material preparation, the prototype was specifically concentrating on educating users on phishing attacks.

The topic was chosen because it is the hot topic in security arena and mostly susceptible to users (Sheng et al. 2007; Robila & Ragucci 2006). The type of KMS to be implemented was determined based on the approach described in section 4.5.2. The approach shows that all education institutions fall under *"Service-based low volatile"* category (Kankanhalli et al. 2003). This implies that the nature of KMS to be implemented for that particular category must be a hybrid of collaborative tools and repositories.

Collaborative tools enable *knowledge providers* to share their understanding on computer threats with *knowledge seekers* (Markus 2001). Moreover, repositories enable *knowledge intermediary* to structure and store knowledge provided into useful

format for future use. However, for the case of this prototype, users play dual roles; both *seekers* and *providers*. They are *seekers* because they need to be aware on current phishing techniques and how to deal with them.

Moreover, they are also *knowledge providers* because they direct computer security personnel what need to be included in awareness materials. However, this is done indirectly by letting users to rank the topics based on their importance. Therefore, from the rank, computer security personnel will be able to understand users' needs and tailor the learning material to the needs. This approach not only attracts many users but also improves material relevance and hence successfulness of security awareness programme(s).

On the other side, computer security personnel play threefold roles; provider, seeker and intermediary (Markus 2001). They are *knowledge providers* because they initiate the learning process by providing users with knowledge of how to protect against phishing attacks. Moreover, they also play as *intermediaries* because they are responsible for codification of their knowledge. Also they are *knowledge seekers* because they are dependant on users to shape learning materials.

The prototype was implemented using an online free powerful Wiki tool, http://kms-sawa.wetpaint.com. Most importantly, it has two unique features that were found to be very useful to the implementation of this prototype; private accessibility and tracking of changes. The tool enables a creation of a private account that can only be accessible to the invited members. This resolved the risk of intruders gaining access as mentioned in the proposal. Moreover it tracks every changes made on pages thus it is useful for monitoring progress of the system.

7.5.1 Prototype descriptions

As it was mentioned previously, this type of prototype is a collaborative KMS to assist knowledge *providers*, *seekers* and *intermediaries* into capturing and sharing security related knowledge. In this KMS there were two actors, *members*/*users* who were academic staff and *security administrator* who was author, under a supervision of security expert. Awareness materials were limited on phishing attacks because of time

limit and complexity nature of preparation. As it was mentioned previously, knowledge *capturing*, *storing* and *sharing* of knowledge management processes, and *collaborative* and *repositories* features of KMS are useful features for the success of KMS in improving security awareness. Therefore, this section focuses on describing SAWA-KMS prototype as a KMS system for improving security awareness in an organisation based on knowledge storing and sharing.

- ***Knowledge capturing and storing***

As it was explained previously, knowledge capturing concentrates on knowledge articulation and codification while knowledge storing concentrates with managing knowledge content. In this prototype knowledge capturing takes two forms. Firstly, is the direct codification of tacit knowledge from security administrator and codification of explicit knowledge from other sources such as public awareness websites and other security forums. Secondly and lastly, capturing of ongoing discussions to determine and prepare security awareness material.

Capturing tools provided by this prototype is EasyEdit and Attachment capabilities as shown in figure 29. EasyEdit allows member of the community to edit the page and add the contents, as shown in figure 30, while Add attachment as shown on the drop down list of figure 29 allows both a member and administrator to attach files for others to share.

Figure 30: Knowledge capturing: Attachments

(Adapted from (http://kms-sawa.wetpaint.com))

Moreover, the prototype provides tagging feature that are useful in organising knowledge contents, see figure 29. For instance in page1 you have included phishing, email scam and identity theft as tags, and in page 2 you have included one of the previous keywords as the tag, when you open either of the pages it the prototype will include the link for the other page. Tags also help when searching for documents. You just need to know the keyword. This is in fact a very useful feature of knowledge storing because it reduce the time members searches for documents.

Figure 31: SAWA-KMS Phishing attacks page

(Adapted from (http://kms-sawa.wetpaint.com))

- ***Knowledge sharing***

Other useful process of knowledge management that was highlighted as useful in using KMS to improve security awareness is knowledge sharing. In this process, knowledge sharing is accomplished by discussion forum facility of the prototype, see figure 32. This facility collaborate members to share different views concerning computer security. The good part of it, which differentiates it from email, is the track-keeping of all previous discussions. It shows who edited the discussion and when it was edited and what contents has been edited. All these are presented in one window called *"Dashboard"*.

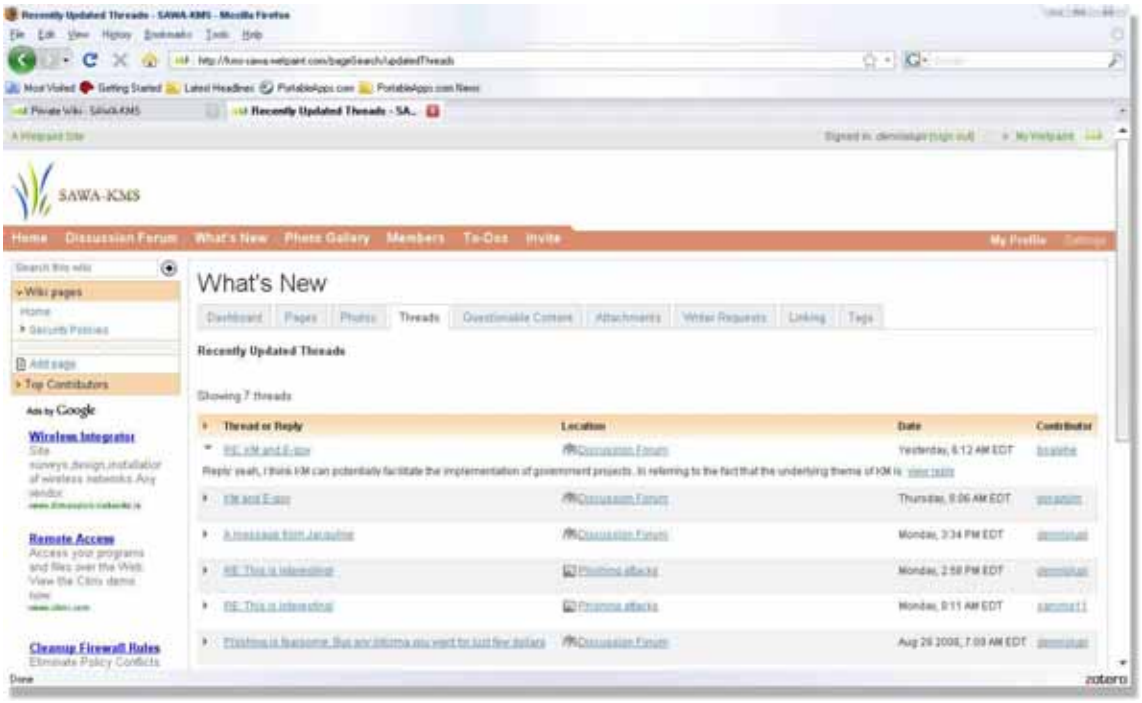

Figure 32: SAWA-KMS threads dashboard

(Adapted from (http://kms-sawa.wetpaint.com))

Alavi and Leidner (1999) ascertain that learning is a process of internalising and converting information to knowledge. Therefore, besides the richness of knowledge content, members' awareness on the content is fundamental to speed up the learning process. Having noticed this illness, the prototype deploys the push-pull strategy to notify members by automatically sending an email about new *"arrival"* so that they can retrieve at their convenient (Nonaka 2005, p.188).

Based on all these features and the considerations taken during its implementation process, this prototype can definitely assisting in security knowledge sharing and hence improve security awareness in an organisation.

7.5.2 Prototype testing

Now that we know what the prototype is capable of, let us now analyse its applicability in industry. As it was explained previously, the prototype has two actors; security administrator and members. Security administrator for initiating and updating security knowledge content and members for participating in security based discussions. The testing of this prototype was done in two phases. Phase one was during the implementation and in phase two is after the implementation.

- ***Testing during prototype implementation***

This was ongoing testing where a number of security experts were invited with administrative privileges of the prototype to monitor on the look and feel of security materials. This included what should be included in what extent under what title. This was a very effective way of presenting security content of the site to make members finds what they expect and hence increase its usability.

- ***Operational testing***

This is the testing after completion of prototype implementation. In this phase members were invited to participate in the prototype. A copy of invitation can be found in appendix C. These members were specifically academicians from Africa so as to get a clear feeling on the contribution of the prototype to their knowledge since Africa symbolises developing countries which are very poor in computer security (ITU 2007).

7.6 Evaluation

Due to poor accessibility of internet services, users' response was very poor. This can evidently shown by the fluctuation shape of the activity diagram as shown in figure 34. However, regardless the poorness of members' accessibility, there are total number of seven knowledge sharing events, see figure 33. This implies that, with time the prototype could be more interactive and increase more knowledge sharing.

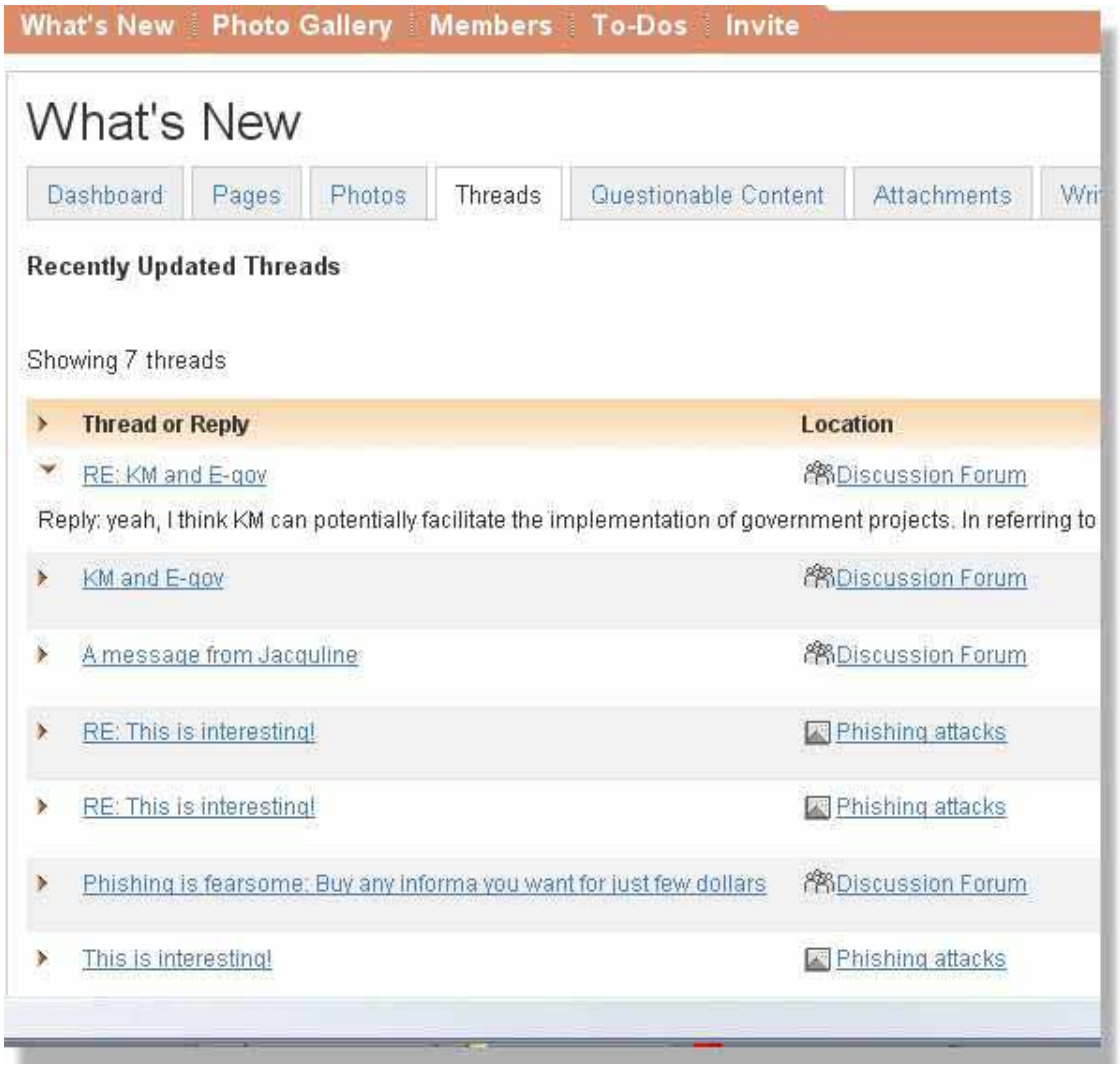

Figure 33: Current Discussions

(Adapted from (http://kms-sawa.wetpaint.com))

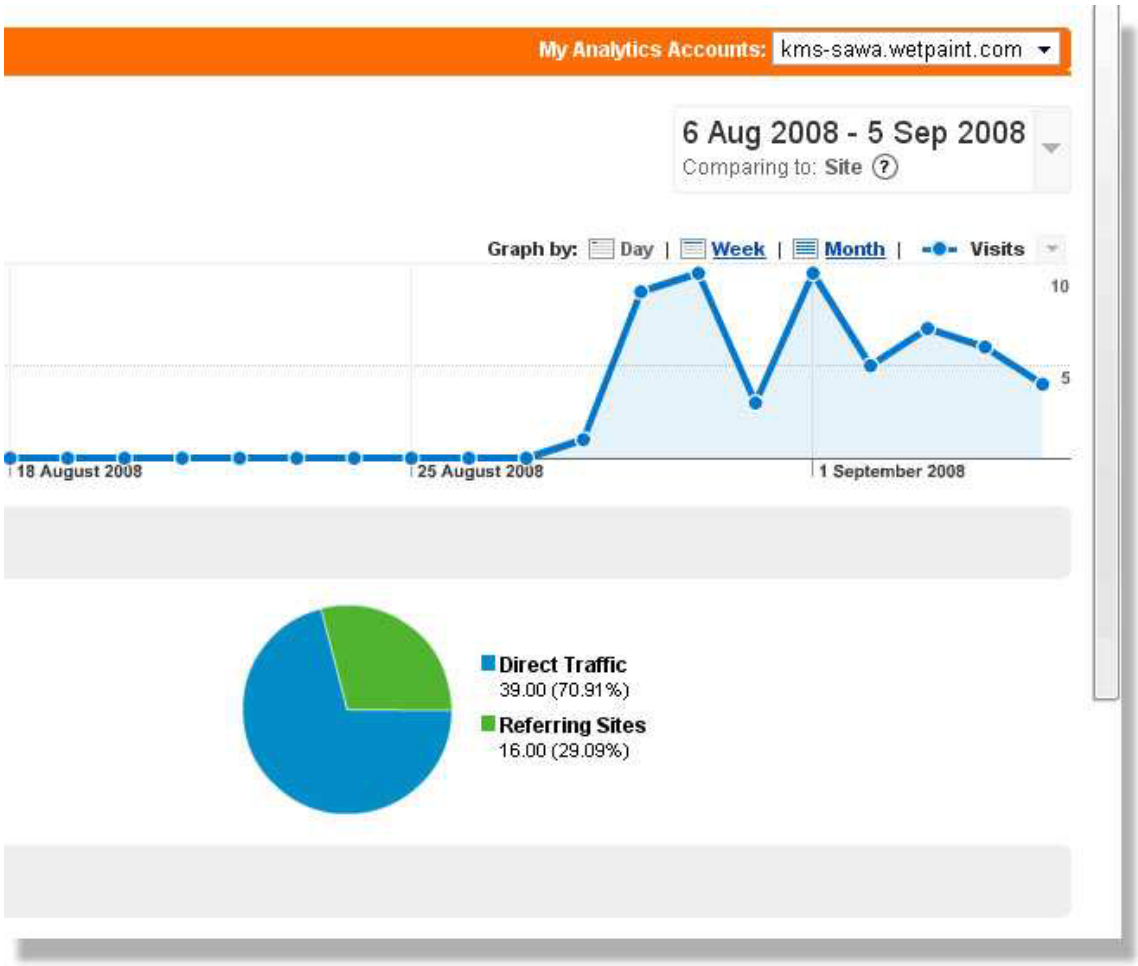

Figure 34: Activity graph

(Adapted from (https://www.google.com/analytics/))

7.7 Conclusion

This chapter aimed at describing the development of a KMS-SAWA framework and the implementation of a Wiki-based prototype. The framework is made up with three factors based on the findings obtained from literature review and security awareness survey. The explanation of these factors was provided in section two. The initial framework was described in section three which was evaluated by security expert to assess its readability and applicability. The evaluation was interview-based. Following the recommendations from security expert, a complete framework was developed. The description of a complete framework was provided in section four where difference phases of KMS implementation were explained.

In section five, the description of Wiki-based prototype was provided. The description of the prototype was based on knowledge capturing, storing and sharing processes of

knowledge management as identified in chapter five. The EasyEdit and attachment facilities of Wiki have been identified to facilitate knowledge capturing. Moreover, the discussion forums and threads have been identified to facilitate knowledge sharing. Both security experts and users were invited to test and evaluate the prototype. The evaluation of the prototype was provided in section six. The following chapter provides the summary of the project and identifying and the recommendation of future work.

8 CONCLUSION

8.1 Introduction

Since now we are approaching to end of this dissertation, it is worthwhile having a quick grasp of what was done up to this end. This chapter will detail the results, conclusions and recommendations reached from the research conducted. The aim of this project was investigate users' awareness in security issues and the usefulness of KMS in improving security user awareness thereafter to develop a framework that leverages KMS in improving security awareness in an organisational context. From this framework a prototype KMS was developed. This chapter will discuss the major results of this project and also recommend future research needed to give a more comprehensive overview of the issues addressed and findings of the project discussed in this dissertation.

8.2 Research Definition & Research Overview

Security awareness is the key issue in the prosperity of organisations. Organisations are heavily reliant on users for their operations and yet users are becoming more susceptible to threat over time. Though there are many technological control measures, users' co-operation is still of particular value. Organisations need to seriously address human issues in security by building security learning environments that will integrate security ethics in their daily operations.

The aim of the project was to investigate users' awareness of computer security issues and the feasibility of employing a KMS to improve security awareness in an organisational context. Thereafter the aim was to develop a framework that leverages KMS to improve security awareness in an organisational context. Finally this project developed a Wiki-based KMS prototype based on the framework developed, which was evaluated by both security experts and end-users with the security experts guiding the development of the prototype while end-users were involved in evaluating the prototype assessing the contribution of the KMS to improving their security knowledge.

8.3 Contributions to the Body of Knowledge

Firstly and foremost the role of users in security and security awareness was identified as the main research area of this project. The motive behind this is the increased rate of security break-ins due to poor understanding of security standards. Following this, KMS was identified as a possible solution to improve security awareness. The motive behind choosing KMS is their success in improving organisation's performance in other knowledge areas.

In order to accomplish this, an extensive literature review on security and security awareness area was undertaken to ascertain current key issues in an organisational context. An extensive exploration of computer security was covered where the trend of security threats and their control measures related to users were explored. Further, an investigation of security awareness was conducted where different security awareness approaches were explored. Although users' involvement in security is an active research area, the literature reveals that little effort has been invested in implementing effective security awareness programmes to combat the problem.

Using the findings from the literature review, a survey was prepared targeting security experts and organisational users, particularly academic users in Africa. The aim of the survey was to investigate the role users' play in computer security and the contributions of current security awareness programmes in educating users. The survey revealed both poor user involvement and limitations in use of security awareness programmes. Moreover, the survey revealed the gap of security perceptions in developed and developing countries.

The aim of this project was to develop a framework to leverage KMS to improve security awareness within an organisation context. To accomplish this, an extensive literature review was also conducted on Knowledge Management and KMS. Knowledge Management involves many processes that have effects on successful implementation of KMS. Therefore it was necessary to have a clear understanding of these processes. Moreover it was necessary to conduct a literature review on KMS so as to ascertain key features that could be leveraged for improving security awareness within an organisation.

Using this, an assessment of knowledge activities and features of KMS that were suitable for improving security awareness was conducted. The assessment revealed knowledge storing and sharing of Knowledge Management processes, and the collaborative and repository features of KMS could be effectively used to improve security awareness among employees within an organisation.

Based on the results from literature reviews and survey, a framework to leverage KMS to improve security awareness was developed. The framework is an open framework that can be deployed in any organisation as guidance in implementing KMS for improving security awareness. The framework was evaluated by security experts and proved to be applicable in an organisation context.

Following the evaluation of the framework, a prototype of KMS was developed using Wiki collaborative tool. The aim of the prototype was to assess the usefulness of KMS on improving security awareness. Many security experts and academic users, specifically from Africa were invited to participate in the Wiki. Security experts were invited to monitor the content of the Wiki during implementation, while users were invited to assess the usefulness of KMS in raising their awareness on computer security.

Although the time was limited, the results obtained reflect the positive effects on using KMS to improve security awareness. Moreover, users from Africa were considered as good system evaluators because, as the survey results revealed, they are not familiar with computer threats. Therefore, KMS will have a direct impact on their knowledge based on computer threats.

8.4 Experimentation, Evaluation and Limitation

The survey conducted as part of this research aimed to investigate the roles of users in computer security and the effectiveness of security awareness programmes in educating users on computer related issues. The survey was conducted in three phases. Phase one was conducted during the ICITST seminar which was conducted on 23rd June 2008. The second phase was conducted in Tanzania on mid July 2008 which

resulted to an extension of the survey to other developing countries such as Kenya and Uganda. The final phase was conducted online. Results obtained from the survey were then evaluated by security experts through a face-to-face interview.

There are many countries that fall under categorisation of developing countries, but due to time limit this survey only concentrated with three countries which are Tanzania, Kenya and Uganda. Similarly, for the developed countries only those countries of the attendees of ICITST 2008 were considered. This limited the range of countries considered during this research however the countries considered can be considered suitable representatives of their categorisation.

Though the result obtained was enough for the development of the framework, still there was limitation on the number of audiences. The response rate from audience was relatively poor especially for online survey. Many audiences were invited to participate in online survey but only few responded to the invitation and only very few completed the survey. Moreover, the survey was conducted in mid June, which was during summer break. Therefore it was difficult to distribute questionnaires and there were many out-of-office notification emails.

Following the results obtained from literature review and survey, a framework was developed to guide the implementation of KMS to improve security awareness in an organisational context. The framework was then evaluated for its applicability by security expert. Thereafter, a Wiki-based prototype was implemented to evaluate the usefulness of KMS in improving security awareness. The prototype was both evaluated by security experts and users from Africa. Security expert was for evaluation of the prototype during its implementation while users were for evaluating the contribution on their security related knowledge.

Due to limitation of internet accessibility, the response from users was relatively poor. This led to limited results during evaluation. To prove the contribution of KMS in improving security awareness a longer timeframe, potentially of years, is required. However, the results obtained from this project have contributed sufficient results to merit more investigation that have already been set a clear, validated pathway to continue.

8.5 Future Work & Research

There are many countries that fall under categorisation of developing countries, but due to time limit this survey only concentrated with three countries which are Tanzania, Kenya and Uganda. Therefore, it is a recommendation of this project to extend this investigation and include more countries that fall under developing so as to gain more insights on their understanding of digital threats and their possible causes.

A valuable extension of this research would be to pick Tanzania as a sample country in developing countries and implement a more functional Wiki based KMS that can be accessible to the public so as to monitor their progress on gain new insights into cultural aspects of digital threats and use the experience and findings to expand this same strategy to other developing countries.

In an organisational context, it would be interesting to implement a similar Wiki-based KMS in a series of organisations of various organisation, technical and security cultures and to monitor the progress of users in gaining new insights on digital threats. The findings of such research would be extremely useful in assessing the robustness of the framework developed by this research and allow it to be extended to be applicable and useful to a broader base. Thereafter it would be possible to extend this research to recommend a series of KMS which could be implemented based on organisational profiles.

8.6 Conclusion

This project highlighted the usefulness of KMS in improving security awareness in an organisational context. From literature review and supporting survey responses, user involvement in computer security decisions was discovered to be very poor. Based on these findings, a framework was developed to guide the implementation of KMS in improving security awareness. Thereafter a Wiki-based prototype was implemented to evaluate the contributions of KMS in improving security awareness.

Moreover, the survey revealed the gap of computer security perceptions between developed and developing countries. This has produced another area of potential research which could be exploiting and extending the findings of this project.

BIBLIOGRAPHY

Alavi, M 1997, KPMG Peat Marwick US: One Giant Brain, *Harvard Business Review: Creating a System to*.

Alavi, M & Leidner, D.E 1999, Knowledge management systems: issues, challenges, and benefits, *Communications of the AIS*, 1(2es).

Allee, V 1997, 12 principles of knowledge management, *Training & Development*, 51(11), 71-4.

Andress, A 2003, *Surviving Security: How to integrate people, process, and technology*, CRC Press.

Andriessen, E & Huis in 't Veld, M 2001, Group dynamics and CoPs.

Arce, I 2003, The weakest link revisited [information security]. *Security & Privacy, IEEE*, 1(2), 72-76.

Benbya, H, Passiante, G & Aissa Belbaly, N 2004, Corporate portal: a tool for knowledge management synchronization. *International Journal of Information Management*, 24(3), 201-220.

Bernard, J 2006, A Typology of Knowledge Management System Use by Teams, In *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on*. p. 155a.

Bishop, M.A 2003, *Computer Security: Art and Science*, Addison-Wesley Professional.

Bishop, M 2005, *Introduction to Computer Security*, Addison-Wesley.

Bixler, C 2002, Applying the four pillars of knowledge management.

Buckley, R & Caple, J 2007, *The Theory & Practice of Training*, Kogan Page.

Bugada, S 2005, State of Cybersecurity in Uganda, Available at: http://www.itu.int/osg/spu/cybersecurity/contributions/Uganda_Bugaba_paper.pdf. [Accessed August 26, 2008].

Building an Information Technology Security Awareness and Training Program. Available at: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf [Accessed September 24, 2008].

Carroll, J.M 1996, *Computer Security*, Butterworth-Heinemann.

Chia, P.A Maynard, S.B & Ruighaver, A.B 2002, Understanding Organizational Security Culture. *Proceedings of PACIS2002. Japan*.

Cole, E 2002, *Hackers Beware*, New Riders.

Cole, K, Chetty, M, LaRosa, C, Rietta, F, Schmitt, D.K, Goodman, S.E & Atlanta, G.A 2008, Cybersecurity in Africa: An Assessment.

Contos, B 2007, Insider threat monitoring is enhanced by asset relevance, *Infosecurity*, 4(2), 47-47.

D'Arcy, J & Hovav, A 2007, Deterring internal information systems misuse. *Communications of the ACM*, 50(10), 113-117.

Davenport, T.H, De Long, D.W & Beers, M.C 1998, Successful knowledge management projects, *Sloan Management Review*, 39(2), 43-57.

Davenport, T.H & Probst, G.J 2002, *Knowledge Management Case Book: Siemens best practices* 2nd ed, Cambridge: John Wiley & Sons.

Denton, J 1999, Organisational learning and effectiveness, Ebrary.

Dervitsiotis, K.N 1998, The challenge of managing organizational change: Exploring the relationship of re-engineering, developing learning organizations and total quality management. *TOTAL QUALITY MANAGEMENT*, 9(1), 109-122.

Desman, M.B 2002, *Building an Information Security Awareness Program*, Auerbach Publications.

Dhillon, G 1999, Managing and controlling computer misuse, *Information Management & Computer Security*, 7(5).

Fairchild, A.M 2002, Knowledge management metrics via a balanced scorecard methodology, *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, 3173-3180.

Falbo, R.A, Arantes, D.O & Natali, A.C 2004, Integrating Knowledge Management and Groupware in a Software Development Environment. In *5th International Conference, PAKM 2004, Vienna, Austria, December 2004 Proceedings*. Springer, pp. 94-105.

Folkens, F & Spiliopoulou, M 2004, Towards an Evaluation Framework for Knowledge Management Systems. , 23-34.

Fyffe, G 2008, Addressing the insider threat. *Network Security*, 2008(3), 11-14.

Gorge, M 2007, Cyberterrorism: hype or reality? *Computer Fraud & Security*, 2007(2), 9-12.

Gronau, N, Muller, C & Uslar, M 2004, The KMDL Knowledge Management Approach: Integrating Knowledge Conversions and Business Process Modeling. In *5th International Conference, PAKM 2004, Vienna, Austria, December 2004 Proceedings*. Springer, pp. 1-10.

Gupta, A & Toong, H 1984, The first decade of personal computers. *Proceedings of the IEEE*, 72(3), 246-258.

Gupta, S & Mccabe, D 1987, Personal Computer Displays. *Computer Graphics and Applications, IEEE*, 7(10), 17-23.

Hahn, J & Subramani, M.R 2000, A framework of knowledge management systems: issues and challenges for theory and practice. *Proceedings of the twenty first international conference on Information systems*, 302-312.

Hansen, M.T, Nohria, N & Tierney, T 2005, What's Your Strategy For Managing Knowledge? *Knowledge Management*, 77(2), 106-16.

Herold, R 2005, *Managing an Information Security and Privacy Awareness and Training*, Auerbach Publications.

http://beta.group-surveys.com/asp/user/mysurveys.asp, Group-Surveys.com. Available at: http://beta.group-surveys.com/asp/user/mysurveys.asp [Accessed August 22, 2008].

http://kmjeff.blogspot.com/2007/07/death-by-e-mail.html, Jeff's KM blog: Death by e-mail. Available at: http://kmjeff.blogspot.com/2007/07/death-by-e-mail.html [Accessed August 22, 2008].

http://www.bbbonline.org/idtheft/phishing_cond.asp, Identity Theft. Available at: http://www.bbbonline.org/idtheft/phishing_cond.asp [Accessed July 22, 2008].

http://www.bmc.com/products/products_services_detail/0,,0_0_0_1301,00.htm, BMC Configuration Management (formerly Marimba). Available at: http://www.bmc.com/products/products_services_detail/0,,0_0_0_1301,00.htm [Accessed August 3, 2008].

http://www.cc.gatech.edu/pixi/images/projectShots/talc.jpg, talc.jpg (JPEG Image, 463x361 pixels). Available at: http://www.cc.gatech.edu/pixi/images/projectShots/talc.jpg [Accessed July 31, 2008].

http://www.cmu.edu/news/images/phil-screenshot.jpg, phil-screenshot.jpg (JPEG Image, 718x540 pixels) - Scaled (68%). Available at: http://www.cmu.edu/news/images/phil-screenshot.jpg [Accessed July 31, 2008].

http://www.iab.ie/, Internet Advisory Board - Home. Available at: http://www.iab.ie/ [Accessed July 30, 2008].

http://www.independent.ie/breaking-news/national-news/minister-launches-internet-security-awareness-campaign-1287215.html, Minister launches internet security awareness campaign - National News, Breaking News - Independent.ie. Available at: http://www.independent.ie/breaking-

news/national-news/minister-launches-internet-security-awareness-campaign-1287215.html [Accessed July 30, 2008].

http://www.makeitsecure.org/en/index.html, makeITsecure. Available at: http://www.makeitsecure.org/en/index.html [Accessed July 30, 2008].

http://www.ncte.ie/InternetSafety/, NCTE (National Centre for Technology in Education) - Internet Safety. Available at: http://www.ncte.ie/InternetSafety/ [Accessed July 30, 2008].

http://www.tanzania.go.tz/pdf/ictpolicy.pdf, 2003. NATIONAL INFORMATION AND COMMUNICATIONS TECHNOLOGIES POLICY. Available at: http://www.tanzania.go.tz/pdf/ictpolicy.pdf [Accessed August 26, 2008].

http://www.watchyourspace.ie/, Watch Your Space. Available at: http://www.watchyourspace.ie/ [Accessed July 30, 2008].

Information Technology Security Training Requirements: A Role- and Performance-Based Model. Available at: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf [Accessed September 25, 2008].

ITU, 2007, Telecommunication/ICT markets and trends in Africa. Available at: http://www.itu.int/ITU-D/ict/statistics/material/af_report07.pdf [Accessed August 26, 2008].

Janczewski, L & Colarik, A.M 2005, *Managerial Guide for Handling Cyber-terrorism and Information Warfare*, Idea Group Publishing.

Kankanhalli, A, Tanudidjaja, F, Sutanto, J & Tan, B.C.Y 2003, The role of IT in successful knowledge management initiatives. *COMMUNICATIONS OF THE ACM*, 46(9), 69.

Kemp, M 2005, Barbarians inside the gates: addressing internal security threats. *Network Security*, 2005(6), 11-13.

Kim, W.C & Mauborgne, R 2003, Fair Process: Managing in the Knowledge Economy. *HARVARD BUSINESS REVIEW*, 81(1), 127-136.

King, W.R, Marks Jr, P.V & McCoy, S 2002, The most important issues in knowledge management. *Communications of the ACM*, 45(9), 93-97.

KPMG, 2000, KPMG KM Research Report 2000. Available at: http://www.providersedge.com/docs/km_articles/KPMG_KM_Research_Report_2000.pdf [Accessed August 17, 2008].

Lang, J.C 2001, Managerial concerns in knowledge management. *Journal of Knowledge Management*, 5(1), 43-57.

Lave, J & Wenger, E 1991, *Situated Learning: Legitimate Peripheral Participation*, Cambridge University Press.

Lee, Y.W. et al., 2002. AIMQ: a methodology for information quality assessment. *Information & Management*, 40(2), 133-146.

Maletic, J.I & Marcus, A 2000, Data Cleansing: Beyond Integrity Analysis. *Proceedings of the Conference on Information Quality (IQ2000), Boston, October*.

Malhotra, Y 2005, Integrating knowledge management technologies in organizational business processes: getting real time enterprises to deliver real business performance.

Markus, M 2001, Toward a Theory of Knowledge Reuse: Types of Knowledge Reuse Situations and Factors in Reuse Success. *Journal of Management Information Systems*, 18(1), 57-93.

Marwick, A.D 2001, Knowledge management technology. *IBM Systems Journal*, 40(4), 814-830.

McClelland, R & Thomas, V 2002, Confidentiality and security of clinical information in mental health practice. *Advances in Psychiatric Treatment*, 8(4), 291-296.

McClure, S, Scambray, J & Kurtz, G 2005, *Hacking Exposed: Network Security Secrets & Solutions*, McGraw-Hill Osborne Media.

McDermott, R 1999, Why information technology inspired but cannot deliver knowledge management. *California Management Review,*, 41, 03-17.

McGraw, G 2004, Software security. *Security & Privacy Magazine, IEEE*, 2(2), 80-83.

Mowery, D.C & Simcoe, T 2002, Is the Internet a US invention?—an economic and technological history of computer networking. *Research Policy*, 31(8-9), 1369-1387.

Nonaka, I 2005, A Dynamic Theory of Organizational Knowledge Creation. *Knowledge Management: Critical Perspectives on Business and Management*, 5(1), 14-37.

Nonaka, I 1994, A dynamic theory of organizational knowledge creation. *Organization Science*, 5(1), 14-37.

Nonaka, I & Takeuchi, H 1995, *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*, Oxford University Press, USA.

Nosworthy, J.D 2000, Implementing Information Security In The 21st Century -- Do You Have the Balancing Factors? *Computers & Security*, 19(4), 337-347.

O'Leary, D.E 2008, Wikis:'From Each According to His Knowledge'. *COMPUTER*, 34-41.

Pfleeger, C.P & Pfleeger, S.L 2003, *Security in Computing*, Prentice Hall PTR.

Randeree, E 2006, Knowledge management: securing the future. *Journal of Knowledge Management*, 10(4), 145-156.

Rao, M 2002, Eight Keys to Successful KM Practice. Available at: http://www.providersedge.com/docs/km_articles/Eight_Keys_to_Successful_KM_Practice.pdf [Accessed August 17, 2008].

Robila, S.A & Ragucci, J.W 2006, Don't be a phish: steps in user education. *Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education*, 237-241.

Rumizen, M 1998, how buckman laboratories' shared knowledge sparked a chain reaction. *The Journal for Quality and Participation*.

Russell, D & Gangemi, G.T 1991, *Computer Security Basics*, O'Reilly Media, Inc.

Sankarpandian, K, Little, T & Edwards, W.K 2008, Talc: using desktop graffiti to fight software vulnerability.

Schifreen, R 2006, *Defeating the Hacker: A Non-technical Introduction to Computer Security*, John Wiley.

Schlienger, T & Teufel, S 2003, Analyzing information security culture: increased trust by an appropriate information security culture. *Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on*, 405-409.

Schultz, E.E 2002, A framework for understanding and predicting insider attacks. *Computers & Security*, 21(6), 526-531.

Schultz, E.E & Shumway, R 2002, *Incident Response: A Strategic Guide to Handling System and Network Security Breaches*, Sams Publishing.

Security Awareness. Available at: http://technet.microsoft.com/en-us/security/cc165442.aspx [Accessed September 25, 2008].

Senge, P.M & Audio, B.D.D 1990, *The fifth discipline*, Doubleday New York, NY;.

Senge, P 1990, *The fifth discipline : the art and practice of the learning organization*, Century Business.

Sharp, R 2007, Internet Safety and Security Surveys–A Review.

Sheng, S, Magnien, B, Kumaraguru, P, Acquisti, A, Cranor, L.F, Hong, J & Nunge, E 2007, Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. *Proceedings of the 3rd symposium on Usable privacy and security*, 88-99.

Siegler, M 2006, Confidentiality in Medicine: A Decrepit Concept. *Bioethics: An Anthology*, 307(24).

Siewiorek, D.P & Swarz, R.S 1998, *Reliable Computer Systems: Design and Evaluation*, A K Peters.

Smith, S 2003, Humans in the loop: human-computer interaction and security. *Security & Privacy, IEEE*, 1(3), 75-79.

von Solms, B 2000, Information Security—The Third Wave? *Computers & Security*, 19(7), 615-620.

Stallings, W 2006, *Cryptography And Network Security: Principles and Practice*, Prentice Hall.

Stanton, J.M, Stam, K.R, Mastrangelo, P & Jolton, J 2005, Analysis of end user security behaviors. *Computers & Security*, 24(2), 124-133.

Stenmark, D 2002, Information vs. Knowledge: The Role of intranets in Knowledge Management. *Proceedings of HICSS*, 35, 7-10.

Straub, D.W & Welke, R.J 1998, Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 22(4), 441-469.

Tanenbaum, A.S 2008, *Modern Operating Systems* 3rd ed., New Jessey: Pearson.

Tochtermann, K, Dosinger, G & Puntschart, I 2004, I-KNOW What You Will Know in Knowledge Management. In *5th International Conference, PAKM 2004, Vienna, Austria, December 2004 Proceedings*. Springer, pp. 35-45.

Trcek, D 2006, Security Models: Refocusing on the Human Factor. *Computer*, 39(11), 103-104.

US-CERT, 2008, The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures. Available at: http://www.cert.org/archive/pdf/08tr009.pdf [Accessed August 28, 2008].

APPENDIX A

Security User Awareness Survey

(Online Questionnaire)

The aim of this survey is to investigate the potential roles users play in information systems security and the effects security user awareness programmes have in educating users on relevant security issues.

All your answers will be confidentially treated. Neither I, Dublin Institute of Technology (DIT) nor any other third party will record your name, email address or any other details that might lead to your identification.

On behalf of Dublin Institute of Technology, I would like to thank you for your contribution in this important survey.

SECTION I
Organisational and Personal Information

Q_1. What is the nature, primary business area of your organisation?

Agriculture	Construction/ Architecture/Engineering	Education	Financial/Banking	Government
Information Technology	Transportation/Logistics	Health	Entertainment	Telecommunications

Others (Please specify):

Q_2. How big is your organisation in terms of the number of employees?

Less than 100	100 – 499	500 – 999	1000 - 4999	5000 – 9999	More than 10000

Q_3. In which country is your organisation located?

_____

Q4. In your opinion, how dependant is your organisation's operations on computer systems?

Don't know	Not at all	Very low	Low	Medium	High	Very high

Comments:

Q5. What best describes your role in your organisation?

CIO for Chief Information Officer, CTO for Chief Technology Officer, CSO for Chief Security Officer and CISO for Chief Information Security Officer.

CIO/CTO	CSO/CISO	IT Manager	Other IT Personnel	System Administrator

Others (Please specify):

Q6. What is your experience in information systems security?

No experience	1 – 5 yrs	6 – 9 yrs	10 – 15 yrs	More than 15 yrs

Q7. Do you have any security professional qualification?

Yes	No

If your answer is "No", please go to section two.

Q8. What security professional qualification(s) do you possess?

CISA	CISM	CISSP	ISSAP	ISSMP	ISSEP	CAP	SSCP

Others (Please specify):

Q9. With your security professional qualification(s), do you think it has helped to raise awareness of your role in/responsibilities for security within your organisation?

Yes	No	Don't know

Comments:

If your answer is "No" or "Don't know", please skip question 10.

Q10. In your opinion, how much has your security professional qualification(s) helped you to contribute to your organisation's information systems security?

Not at all	Very low	Low	Medium	High	Very high

Comments:

SECTION II
Roles of users in information systems' security

Q1. Are there any security policies in your organisation?

Yes	No	Don't know

Comments:

If your answer is "No" or "Don't know", please skip question 2, 4, 15, 16 and 17.

Q2. In your opinion, how involved are end-users in establishing security policies in your organisation?

Don't know	Not at all	Very low	Low	Medium	High	Very high

Comments:

Q3. Is there any roles/designation other than administrators that requires computer administrative privileges to perform their tasks?

Yes	No	Don't know

Comments:

If your answer is "No" or "Don't know", please skip question 4.

Q4. Does your organisation's security policy include policy on restrictions of applications installation??

Yes	No	Don't know

Comments:

Q5. In your opinion, how involved are users in operating your organisation's computer systems?

Don't know	Not at all	Very low	Low	Medium	High	Very high

Comments:

Q6. In your opinion, how involved are users in designing your organisation's information systems?

Don't know	Not at all	Very low	Low	Medium	High	Very high

Comments:

Q7. In your opinion, how involved are users in developing your organisation's information systems?

Don't know	Not at all	Very low	Low	Medium	High	Very high

Comments:

Q8. In your opinion, how involved are users in configuring your organisation's information systems?

Don't know	Not at all	Very low	Low	Medium	High	Very high

Comments:

Q9. In your opinion, how knowledgeable are end-users in social engineering computer attacks?

Don't know	Not at all	Little knowledgeable	Knowledgeable	Highly knowledgeable

Comments:

Q10. In your opinion, how knowledgeable are end-users on technical computer attacks?

Don't know	Not at all	Little knowledgeable	Knowledgeable	Highly knowledgeable

Comments:

Q11. Do you think it is necessary to educate end-users on information systems security matters?

Yes	No

Comments:

Q12. In your opinion, how knowledgeable are IT Personnel in information systems' security attacks?

Don't know	Not at all	Little knowledgeable	Knowledgeable	Highly knowledgeable

Comments:

Q13. Do you think it is necessary to educate IT Personnel on information systems security matters?

Yes	No

Comments:

Q14. In your opinion, how interactive are IT Personnel with end-users?

Don't know	Not at all	Very low	Low	Medium	High	Very high

Comments:

Q15. In your opinion, how much do end-users adhere with security policies within your organisation?

Don't know	Not at all	Very low	Low	Medium	High	Very high

Comments:

Q16. In your opinion, how much do IT Personnel adhere with security policies within your organisation?

Don't know	Not at all	Very low	Low	Medium	High	Very high

Comments:

Q17. In your opinion, how contributive security policies are in ensuring security of your organisation's information systems?

Don't know	Not at all	Very low	Low	Medium	High	Very high

Comments:

Q18. Does your organisation have any motivation scheme to attract end-users to practice good security principles?

Yes	No

Comments:

SECTION III
Impact of Security User Awareness Programmes

Q_1. Does your organisation have any security user awareness programme?

Yes	No	Don't know

Comments:

If your answer is "No" or "Don't know", please go to question 10, 12 and 13.

Q_2. What form of security user awareness programme(s) does your organisation practice?

Web-based	Posters	Presentations	Email	Face-to-face	Don't know

Others (Please specify)

Q_3. Does your organisation's security user awareness programme(s) go beyond awareness of security policies?

Yes	No	Don't know

Comments:

If your answer is "No" or "Don't know", please skip question 4.

Q_4. If it goes beyond awareness of security policies, do you think it matches with the dynamic nature of computer security threats?

Yes	No	Don't know

If yes, how?

Q5. Are IT personnel among the targeted users of your security user awareness programme(s)?

Yes	No	Don't know

Comments:

If your answer is "No" or "Don't know", please skip question 7.

Q6. In your opinion, how responsive are end-users to security user awareness programme(s)?

Not at all	Very low	Low	Medium	High	Very high

Comments:

Q7. In your opinion, how responsive are IT Personnel to security user awareness programme(s)?

Not at all	Very low	Low	Medium	High	Very high

Comments:

Q8. Does your security user awareness programmes contribute to a decrease in information systems security attacks?

Yes	No	Don't know

Comments:

Q9. In your opinion, how relevant are security user awareness materials to the targeted users within your organisation?

Don't know	Irrelevant	Moderate	Relevant

Comments:

Q10. Does your organisation have computer security logging activated?

Yes	No	Don't know

Comments:

If your answer is "No" or "Don't know", please skip question 11.

Q11. Does your security user awareness programme(s) material consider audited/logged information?

Yes	No	Don't know

Comments:

Q12. In your country, are there any legal requirements for educating users in security issues?

Yes	No	Don't know

If yes, please specify:

If your answer is "No" or "Don't know", please skip question 13.

Q13. In your opinion, how much do legal requirements contribute to the security of organisation's information systems?

Not at all	Very low	Low	Medium	High	Very high

Comments:

APPENDIX B

Q_1. "Users' involvement in security policy establishment is directly proportional to their adherence with security policies."

Comments:

Q_2. What is your opinion on consulting users when preparing security awareness materials?

Comments:

Q_3. "Clear understanding of ***organizational culture*** determines the successfulness of security awareness programme"

Comments:

Q_4. "The level of computerization in an organization determines the understandability of information security"

Comments:

Q_5. "Clear understanding of ***organizational security culture*** determines the successfulness of security awareness programme"

Comments:

APPENDIX C

Hi all!

If you remember early July this year you helped me with the completion of security awareness survey. It is my honor to acknowledge your contributions.

The survey was globally hence many countries participated including USA, UK, China, Germany, Nigeria, Kenya, Uganda and many other countries.

However, it is sad to say from all these countries, including our neighbors Kenya and Uganda, our country is the least in computer security understanding.

Following this finding, I have developed a collaborative Knowledge Management System that will enable us to raise our understanding on computer security relevant issues. The system is easy to use and allows you to add and edit any page as you wish, attach documents and above all it enables us to conduct discussions.

This system is designed to operate in an organization environment. However, due to computer security being a national problem, its accessibility with time, will eventually be made public to citizens so as they can also participate in security knowledge sharing thus raise their computer security awareness.

Though the system is in its dawn, with your cooperation we can make it successfully inherited in our society. Participate in this motivation and you will eventually enjoy the fruits of your participation. Let us join power and take this responsibility of educating our nation about security issues.

You may wonder why there are so many dead links, but this is to make you play your part. I have chosen my wing, so you choose yours or go along with me. I welcome your comments about the page, and if you find anything that is missing you can add it.

Following this welcome note, I'll send each member their login credentials individually.

Thanks very much.

Regards,